[SafeGuard® Easy]

[Data protection by encryption]

Version 4.50.3

Windows® Server 2003
Windows® XP
Windows® 2000

utimaco®
safeware

All rights reserved.

No part of this documentation may be reproduced or processed, copied, distributed by a retrieval system in any form (print, photocopies or any other means) except for personal use without prior written consent of Utimaco Safeware AG.

Utimaco Safeware AG reserves the right to modify or supplement the documentation at any time without previous announcement. Utimaco Safeware AG is not liable for misprints and damage resulting from this.

CryptoServer and SafeGuard are registered marks of Utimaco Safeware AG.

Windows, Windows NT, Windows 2000, Windows XP, Windows 2003 Server and Windows CE are registered marks of Microsoft Corporation.

Patents rights of Ascom Tech Ltd. given in EP, JP, US. IDEA is a Trademark of Ascom, Tech Ltd.

All other brand and product names mentioned in this manual are marks of the respective owners and are recognized as such.

Microsoft, Windows, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Utimaco Safeware AG
P.O. Box 20 26
DE-61410 Oberursel
Phone +49 (61 71) 88-0
Fax +49 (61 71) 88-10 10
info.pds@utimaco.com

www.utimaco.com

© Utimaco Safeware AG, 2008

Technical Support

Online Documentation

Our knowledge database provides answers to many typical questions about the SafeGuard product range, including its functionality, implementation, administration and troubleshooting.

Link to support area: http://www.utimaco.com/myutimaco

To access the public area of the knowledge database you can logon as a guest user. To access the restricted area of the knowledge database you need a valid software maintenance agreement. Our support staff continually adds to the contents of both areas, and keeps them up to date on an on-going basis.

Advanced support services and telephone support

For customers with a valid maintenance contract, qualified support staff is available to provide advice and assistance. To receive a contract offer tailored to your specific needs, please contact your Utimaco sales partner.

We hope you understand that some enquiries from customers without a maintenance agreement may require several working days to process. In urgent cases, please contact the Utimaco sales partner from whom you bought your licenses or software subscription.

1 Overview 1

1.1 Central security functions 2
1.2 Other security functions 4
1.3 New features in SafeGuard Easy 10
1.4 Changes to previous versions 12
1.5 System requirements 13
1.6 Documentation 16
1.7 General notes 16
1.8 License note 18

2 Getting started 19

2.1 Preparing for installation 19
2.2 Installation prerequisites 21
2.3 Installable modules 22
2.4 User interface language 23

3 Local installation 25

3.1 Step by step 26
3.1.1 Encryption mode 31
3.2 After installation 33
3.3 Displaying encryption progress 34
3.3.1 Switching off the status screen 34
3.3.2 Defining encryption speed 35
3.4 Changing the background bitmap in the Windows logon dialog 38

3.5 Installing SafeGuard Easy on a PC with multiple operating systems 40

4 Central installation 41

4.1 Creating the configuration file 42

4.2 Installation with Active Directory 43
4.2.1 Prerequisites 43
4.2.2 Using an editor to modify MSI files 44
4.2.3 Deploying MSI files 46

4.3 Installation without Active Directory 48
4.3.1 Command line syntax for unattended installation 49
4.3.2 Selected options used by Windows Installer 51

4.4 SafeGuard Easy features and parameters 52
4.4.1 SafeGuard Easy features 52
4.4.2 SafeGuard Easy setup parameters 55

5 Update 59

5.1 Local update 60

5.2 Unattended update with migration file 64

5.3 System kernel check when there is an update 66
5.3.1 What happens if the system kernel is not OK? 67
5.3.2 About the repair program 68
5.3.3 Parameters for the repair program 69

6 Uninstallation 73

6.1 Local uninstallation 74

6.2 Uninstall with Challenge/Response 75

6.3 Unattended uninstall with configuration file 77

7 System boot and logon 79

7.1 Logging on as a regular user 80

7.2 Logging on as a default user 81

7.2.1 Extended logon via function key [F2] 82

7.3 Logging on using a token 83

7.4 Changing the SafeGuard Easy password via the [F10] key 84

7.5 Help function for resetting forgotten passwords via the [F9] key 85

7.6 Failed logon 86

7.7 Pressing [F2] to force logon with PBA 87

7.8 Logging on to the operating system automatically 88

7.9 Compatibility with logon components supplied by other vendors 89

8 Administration overview 91

8.1 Separation of functions 92

8.2 Starting the Administration function and the Configuration File Wizard 93

8.3 The Administration function..... 94
8.3.1 Administration window 95
8.3.2 Toolbar 96

8.4 Configuration File Wizard 98
8.4.1 Reuse of configuration files from older versions of SafeGuard Easy..... 99
8.4.2 Creating a new configuration file 100
8.4.3 Creating a configuration file for installation .. 101
8.4.4 Creating a configuration file for removing SafeGuard Easy..... 105
8.4.5 Creating a configuration file for a change installation ("delta file")..... 106
8.4.6 Run the delta file..... 110
8.4.7 Changing a configuration file 111

8.5 Command line syntax for creation of a configuration file..... 112
8.5.1 Examples of use 114

8.6 Changing frequently-used Registry settings with SafeGuard Easy's administrative template..... 117

9 Pre-Boot Authentication (PBA)..... 121

9.1 Changing the language used in pre-boot authentication at a later point in time 122

9.2 Switching on password at system start (PBA).... 123

9.3 Machine identification..... 124
9.3.1 Machine identification..... 125

9.3.2 Legal notice 126

10 Master Boot Record 127

10.1 MBR protection 129

10.2 MBR default actions 130

10.3 Support Compaq Setup partition 130

11 Encryption 131

11.1 Configuring encryption 133

11.2 Supported disk drives 134
11.2.1 Encrypting disk drives 138

11.3 Keys 140
11.3.1 Key management 140
11.3.2 Creating keys 140
11.3.3 Key length 141
11.3.4 Trivial keys 141
11.3.5 Random keys 141
11.3.6 Defining keys 142
11.3.7 Changing a key 142

11.4 Algorithms 143
11.4.1 Selecting an algorithm 143
11.4.2 SafeGuard Easy algorithms 143
11.4.3 Changing an algorithm 145

11.5 Displaying encryption status in Windows Explorer 146

11.6 Creating an image of an encrypted hard disk drive 147

12 Creating user profiles 149

12.1 Defining admin tasks 150

12.2 Pre-defined users 151
12.2.1 The SYSTEM user 151
12.2.2 The USER user 151
12.2.3 The *AUTOUSER 152

12.3 Creating users 153

12.4 Copying a user 154

12.5 Deleting users 155

12.6 User features 156
12.6.1 Minimum user name length 156
12.6.2 Token logon 157
12.6.3 Default user (password only) 157
12.6.4 Issue abbreviated C/R Code 157
12.6.5 User account template 158
12.6.6 Expiration date 159

12.7 User rights 160
12.7.1 Assigning user rights 162
12.7.2 Transferring user rights 163

13 Password settings 165

13.1 Pre-defined password rules 166

13.2 Permitted keys for the SafeGuard Easy password 167

13.3 Configuring SafeGuard Easy for use in international environments 168
13.3.1 The effects of different keyboard layouts 168
13.3.2 Generating internationally uniform data for SafeGuard Easy 169

13.4 General password rules 171
13.4.1 Password at system start..... 172
13.4.2 Hidden password entry 172
13.4.3 Minimum password length 172
13.4.4 Minimum password age..... 172
13.4.5 Password history..... 173
13.4.6 Syntax rules (characters, digits, symbols, opposite case)..... 174

13.5 Forbidden passwords 175
13.5.1 Defining forbidden passwords..... 175
13.5.2 Importing a password list..... 176

13.6 User-specific password rules 177
13.6.1 Password change allowed..... 178
13.6.2 Password change after..... 178
13.6.3 Change password at next logon 178

13.7 Defining a password 179

14 Twinboot/Boot Manager 181

14.1 Functionality..... 181

14.2 Prerequisites 182

14.3 Example..... 183

14.4 Configuring Twinboot 184

14.5 Configuring Boot Manager 186
14.5.1 General settings..... 186
14.5.2 Boot drives..... 187

14.6 Exchanging data between boot partitions (Share Plain Partitions)..... 190

15 Token support 191

15.1 Benefits of logging on using a token 192

15.2 Supported tokens 194

15.3 Token functions 195

15.4 Install token support 196

15.5 Logging on for the first time with a token in the pre-boot authentication 199

15.6 How to change the token password 201

15.7 How to change or delete SafeGuard Easy access data 201

15.8 Issuing a token 202
15.8.1 Token issuing mode 203
15.8.2 Unattended issuing 204

15.9 Token support for SafeGuard Easy Administration Tools 210
15.9.1 Enabling logging on to the Administration Tools with a token 211
15.9.2 Registering the token's PKCS#11 module 212
15.9.3 Universal Token Interface 215

15.10 Logging on to the operating system with token 218
15.10.1 Issuing a token with operating system data 218
15.10.2 Saving Windows data in the SAL file 220

15.11 Issuing a token with the Token Administration 221
15.11.1 Installing the Token Administration 222
15.11.2 Removing SafeGuard Easy data from the token 223
15.11.3 Importing the SafeGuard Easy data from a configuration file 224

15.12 Quickly changing the SafeGuard Easy user 226
15.12.1 Prerequisites 226
15.12.2 Example 227

15.13 Remote help 228
15.13.1 Prerequisites for Challenge/Response 229
15.13.2 Challenge/Response examples 229
15.13.3 Administering token remotely with the Token Administration 234

16 Lenovo Fingerprint Sensor 237

16.1 Requirements 238

16.2 Supported hardware 239

16.3 Installing Lenovo fingerprint support 241

16.4 Changing the SafeGuard Easy password 245

16.5 Frequently asked questions 247

17 Configuring Windows logon 249

17.1 Secure Automatic Logon (SAL) 250
17.1.1 Installing Secure Automatic Logon (SAL) 251
17.1.2 Secure Automatic Logon with smartcard (Smartcard SAL) 254
17.1.3 Switching Secure Auto Logon off temporarily 256
17.1.4 Hiding the SAL dialog 258
17.1.5 Removing data for SAL/SCSAL 259
17.1.6 Restriction 260

17.2 Logging onto Windows and SafeGuard Easy using the same password (password synchronization) 261
17.2.1 Benefits of password synchronization 261

17.2.2 Preparing for password synchronization 262
17.2.3 Switching on password synchronization 263
17.2.4 Carrying out password synchronization 264
17.2.5 Changing the Windows password when password synchronization is active 267
17.2.6 Changing the SafeGuard Easy password 268
17.2.7 Cancelling the password synchronization dialog 269
17.2.8 Restrictions 270
17.2.9 What should I do, if 272

17.3 Additional Windows Logon options 273
17.3.1 Tailoring the Windows Logon screen 274
17.3.2 Workstation lock 277
17.3.3 Screen saver 279
17.3.4 GINA repair 282
17.3.5 Novell logon 283

18 SafeGuard Easy workstation lock 285

18.1 Prerequisites 286

18.2 Activating the Windows Screen Saver with password protection 287

18.3 Switching off the SafeGuard Easy workstation lock 288

19 Secure Wake-On-LAN 289

19.1 Overview 290

19.2 Locking the Windows Logon 291

19.3 Adjusting WOL dialog 292

19.4 Temporary removal of Wake-On-LAN locks 293
19.5 Configuring Wake-On-LAN 294

20 Hibernation 295

20.1 Overview 295
20.2 Hibernation and SafeGuard Easy 296
20.3 Prerequisites and restrictions 297
20.4 Setting up hibernation 298

21 Toggling floppy disk and device encryption 299

21.1 Necessary user rights 300
21.2 Switching encryption 301
21.3 Assigning keys with SgeCrypt 302
21.4 Using the command line to switch encryption settings 304
21.5 Notes 305

22 FIPS 140-2 (Level 1) certification 307

22.1 New functions 308
22.2 Installing SafeGuard Easy to be FIPS-compliant 309
22.3 Secure use of SafeGuard Easy in certified configuration 311

23 SafeGuard Easy and Lenovo ThinkVantage Technologies - Embedded Security Subsystem (Lenovo ESS Chip) 313

23.1 SafeGuard Easy and TPM 315

23.2 Preparing the ESS/TPM Chip for use 316

23.3 Required settings for CSS integration 317

23.4 Required settings for generating random keys using TPM Chip 320

23.5 Required settings for using the TPM chip to secure the Client/Server Authentication 321

23.6 Required settings for Machine Binding 325
23.6.1 Initial Machine Binding 326
23.6.2 Machine Binding failed 328
23.6.3 Machine Binding recovery 329
23.6.4 Recovery mode configuration 332

24 SafeGuard Easy and Lenovo ThinkVantage Technologies - Rescue and Recovery 335

24.1 Overview 335

24.2 Rescue and Recovery with SafeGuard Easy 336
24.2.1 Advantages of combining Rescue and Recovery™ and SafeGuard Easy 337
24.2.2 Requirements 337

24.3 Installation 338
24.3.1 When neither Rescue and Recovery nor SafeGuard Easy are installed 339
24.3.2 SafeGuard Easy is already installed 340

24.4 Upgrade 341
24.4.1 Upgrading SafeGuard Easy 341
24.4.2 Upgrading Rescue and Recovery 341

24.5 Uninstallation 341

24.6 How to create a backup 342

24.7 Restoring file backups 344

24.8 Restoring the system 345
24.8.1 Boot environment 346
24.8.2 Restoring a SafeGuard Easy system 347

24.9 Service and factory recovery partitions 347
24.9.1 Features 348

24.10 What should I do, if 349

25 Compatibility with Absolute Computrace software 351

26 Remote maintenance (Challenge/Response) 353

26.1 How it works 354
26.1.1 Installing PDA version of the Response Code Wizard 355

26.2 Generating a challenge code 356

26.3 Response Code 358
26.3.1 Creating a response code 359

26.4 Optional extensions of the Challenge/Response concept 367
26.4.1 Helpdesk Console 367
26.4.2 Web Self Help 368
26.4.3 VOICE.TRUST 369

27 Creating emergency media and saving the system kernel 371

27.1 How to create an emergency floppy/system kernel backup 372
27.1.1 Running the emergency disk wizard 373
27.1.2 Using the command line to save the system kernel 376
27.1.3 How to save SafeGuard Easy emergency files to floppy 376

27.2 How to create a bootable emergency disk 377

27.3 How to create a bootable emergency CD 378

27.4 How to create a bootable emergency USB memory stick 379

27.5 Performing an emergency boot 380
27.5.1 Restoring a system kernel 381
27.5.2 Repairing the system kernel 382
27.5.3 Emergency uninstall of SafeGuard Easy 383
27.5.4 Notes 385

27.6 Accessing encrypted data when booting from an external medium 386
27.6.1 Prerequisites 387
27.6.2 Procedure 388
27.6.3 Notes 389
27.6.4 What should I do, if 390

28 Displaying SafeGuard Easy system status ... 391

28.1 Reporting 391

28.2 Parameters 392

29 Auditing 393

29.1 How to use Auditing 394

29.2 Installing Auditing 395

29.3 Configuring Auditing 396

29.4 Configuring Event Logging 397
29.4.1 Defining destinations 397
29.4.2 Creating a new destination 399
29.4.3 Removing a destination 400
29.4.4 Copying a destination 400

29.5 Selecting events 401
29.5.1 Configuring all events 403
29.5.2 Changing the view 404

29.6 Viewing audited events 405
29.6.1 Event Viewer 406
29.6.2 Log file 408

29.7 Notes 409

30 Central administration 411

30.1 Functionality 412
30.1.1 SafeGuard Easy Server/ SafeGuard Easy Database 414
30.1.2 SafeGuard Easy Administration Console 416
30.1.3 SafeGuard Easy Clients 417
30.1.4 Supported SafeGuard Easy Client-/ SafeGuard Easy Server combinations 418

30.2 Exchanging Data between Client and Server 419
30.2.1 Secure communication 419
30.2.2 Expected network load 421
30.2.3 Defining the interval for data exchange 422

30.3 Installation 424
30.3.1 Installing SafeGuard Easy Server/Database.... 425
30.3.2 Installing SafeGuard Easy's Administration Console 427
30.3.3 Installing SafeGuard Easy Clients..... 428
30.3.4 Maximum capacity of the SafeGuard Easy Database 431
30.3.5 Restoring a SafeGuard Easy Server or Database 432

30.4 Microsoft SQL Server support 433
30.4.1 Important information..... 433
30.4.2 Generating an empty SafeGuard Easy database on the SQL Server 434
30.4.3 Registering the new (empty) SafeGuard Easy Database on the SafeGuard Easy Server 440

31 Administration Console..... 447

31.1 Logging on to the Administration Console 447
31.1.1 Changing the access data for the database.. 449

31.2 Admin Console user interface..... 451
31.2.1 Saving the contents of a tab as a text file..... 453

31.3 Displaying the current configuration of a SafeGuard Easy Client 454
31.3.1 Changing a SafeGuard Easy Client description..... 455
31.3.2 Removing a SafeGuard Easy Client..... 455

31.4 Re-registering a SafeGuard Easy Client 456
31.4.1 Re-registering several SafeGuard Easy Clients 460

31.5 Registering SafeGuard Easy Clients on another SafeGuard Easy Server 461

31.6 Defining groups 466
31.6.1 Creating/deleting groups 467
31.6.2 Assigning a SafeGuard Easy Client to a group/removing a SafeGuard Easy Client from a group 467
31.6.3 Finding out group membership 468
31.6.4 Changing a group name 469
31.6.5 Removing groups 469

31.7 Defining rules for displaying workstations/groups/requests 469
31.7.1 Configuring a filter 470
31.7.2 Activating a filter 472

31.8 Requests and Queues 472
31.8.1 Creating changes (requests) 474
31.8.2 Creating a new request 475
31.8.3 Using an existing configuration file as a request 476
31.8.4 Failed requests 477
31.8.5 Changing a request name 478
31.8.6 Deleting a request 478
31.8.7 Displaying a queue 478

31.9 State of a SafeGuard Easy Client 480
31.9.1 State "Standard (Online)" 481
31.9.2 State "Offline" 482
31.9.3 State "Push [on]" 483
31.9.4 State "Push [off]" 484
31.9.5 Switching the SafeGuard Easy Client from Standard (Online) to Offline mode 485
31.9.6 Generating configuration updates for offline clients in the Administration Console 487
31.9.7 Loading a configuration update onto an Offline Client with SGETRANS 490

31.10 Automatic system kernel backup 491
31.10.1 Backing up the system kernel into the Backups folder 492
31.10.2 Creating a new backup folder 493
31.10.3 Exporting the system kernel 493

32 Remote Administration 495

32.1 Prerequisites 496

32.2 Installing Remote Administration 498

32.3 Establishing a connection to a SafeGuard Easy Client 500

33 Error messages 503

1 Overview

Personal computers often contain personal data, confidential and company information or other sensitive data.

The danger caused by the theft of notebooks should not be underestimated. Highly sensitive client information on a sales representative's notebook could fall into the hands of a competitor, resulting in serious damage for the company.

SafeGuard Easy is the ideal way to safeguard against such risks without spending too much time on implementing security measures.

How does SafeGuard Easy protect workstations against unauthorized access? The program's most important security features are its drive encryption and boot protection, which are used to prevent access to a workstation via an external data medium.

The biggest benefits of SafeGuard Easy are that the program

- simply but effectively protects the confidentiality of stored data
- can be implemented quickly
- is very user-friendly
- offers a security concept suitable for many different application areas.

SafeGuard Easy is easy to install. For this reason, it is particularly well suited for stand-alone systems and mobile units such as notebooks.

1.1 Central security functions

Encryption

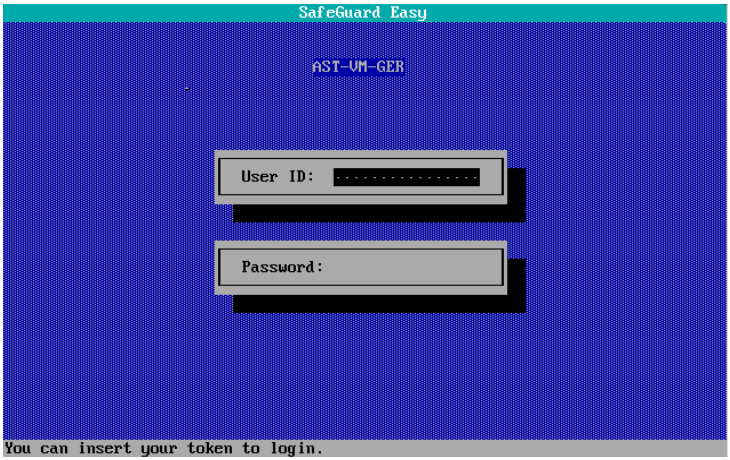
SafeGuard Easy uses online encryption to protect the confidentiality of data that is stored on hard disks, floppy disks and removable media in a simple and effective manner. Here, "online" means that the data is decrypted, when it is read and loaded into RAM, and then automatically encrypted again when it is saved. The key is not saved on the hard disk or PC. It is determined again, from the user's SafeGuard Easy password, each time the PC is switched on.

SafeGuard Easy encrypts not only the entire contents of hard disks, but also the contents of removable media such as floppy disks, ZIP or JAZ disks or USB memory sticks. This allows secure data medium exchange to be implemented within the company, while simultaneously protecting the contents of mobile data media against unauthorized access. It also provides an effective way of preventing the unauthorized importing of data such as unlicensed software or viruses via removable media, since users without the appropriate authorization cannot use plain text media.

Different algorithms can be selected to encrypt floppy disks, removable media and the individual partitions on hard disks. The algorithms that can be used for this purpose include AES, Rijndael, XOR, STEALTH-40, IDEA, BLOWFISH, DES and 3DES.

Access control with Pre-Boot Authentication (PBA) and boot protection

Pre-Boot Authentication is an additional central security function in SafeGuard Easy. PBA ensures that only the SafeGuard Easy user who is registered on the system can log onto it.



When the hard disk is encrypted, any attempt to boot the computer from another data medium, such as a system floppy disk, a CD-ROM or another hard disk, will fail: the hard disk remains blocked. In fact, this means that the system actually does boot, but it is not possible to read the encrypted data on the hard disk.

When PBA is implemented on a workstation along with the Boot protection option, the workstation cannot been booted with an external data medium unless the user knows the correct SafeGuard Easy user data.

1.2 Other security functions

Support for Lenovo's (IBM's) ThinkVantage technologies - Client Security Solution (CSS) 8.10 and Rescue and Recovery 4.20
SafeGuard Easy already supports earlier versions of Lenovo's ThinkVantage technologies. The current version of SafeGuard Easy is still compatible to Lenovo's Client Security Solution (CSS) and Rescue and Recovery (RnR).

Rescue and Recovery (RnR): SafeGuard Easy supports Lenovo's Rescue and Recovery. This means customers can use this efficient backup and recovery method along with SafeGuard Easy encrypted operating system partitions. This functionality is unique amongst disk encryption products. Backups from encrypted SafeGuard Easy systems can be stored on any disk drive used by RnR. Therefore, in an emergency, a system can be restored by loading a backup from CD/DVD, a network drive, a second internal hard disk or a USB hard disk or stick.

TCPA/TPM support (ESS chip/CSS): SafeGuard Easy is the first hard disk encryption product to use the security chips, specified by the Trusted Computing Group (TCG), that are nowadays integrated in the latest notebooks. Among other things, SafeGuard Easy uses these chips to secure the link between the client and administration server, and also to generate random numbers. Naturally, SafeGuard Easy's Secure Auto Logon (SAL or SSO) function can also be used to provide optimum integration in the ESS chip infrastructure.

Certification to FIPS 140-2 Level 1
SafeGuard Easy now complies with the guidelines of FIPS 140-2 Level 1 (FIPS= Federal Information Processing Standard) certification set out by the American National Institute of Standards and Technology (NIST). NIST defines the security criteria for encryption products used by the American government.

SafeGuard® Easy is already certified in accordance with the Common Criteria standard, Evaluation Assurance Level 3 (EAL 3).

Optional two-factor authentication in the Pre-Boot phase
SafeGuard Easy can be configured in such a way that only users with an appropriate token can access the PC. Besides being used in Pre-Boot Authentication (PBA), the token can also, of course, be used at operating-system level for other, certificate-based applications, via the PKCS#11 or CSP standard. Furthermore, the token can also be used by the SafeGuard Easy administrator to log on to the administration programs. SafeGuard Easy users who have forgotten their password or token can be helped by a central help desk.

SafeGuard Easy supports

- various Aladdin eTokens
- Verisign USB token
- RSA SecurID 800 token

Biometric logon with Lenovo Fingerprint Sensor
In addition to logon with USB token (RSA, Aladdin), SafeGuard Easy also supports logon via "fingerprint" in the pre-boot authentication phase. The benefit of using a fingerprint is that a user does not have to remember SafeGuard Easy passwords or the PIN for a USB token. They can identify themselves to a Lenovo notebook, for example, simply by passing their finger over the sensor that is installed on it.

Hibernation (Suspend to Disk) support
This is especially useful for mobile device users who usually avoid booting by simply "pausing" and then later "restoring" their current work session, because these options are provided by modern operating systems. In contrast to most other hard disk encryption products, SafeGuard Easy supports use of hibernation mode, even encrypting the generated image data in order to store it securely on the hard disk. This provides round-the-clock security, reduces power consumption and saves users time, in comparison with normal boot procedures that are currently in use.

Compatibility with Absolute's Computrace software
When Computrace is installed, a stolen computer can report its location via a network. SafeGuard Easy has been prepared to ensure it is compatible with Computrace. This compatibility with SafeGuard Easy means that this feature also works with encrypted hard disks.

Full compatibility requires a version of Computrace Software that, at present (12/2008)) has not yet been released by Absolute Software.

Web Self Help
SafeGuard Easy's Self-Help enables an ordinary user to help themselves if they forget their SafeGuard Easy password. This will lead to an overall decrease in the number of help desk calls that are solely due to forgotten passwords, and therefore the help desk personnel will have more time to work on more complex support cases. There are also various solutions for Challenge/Response in a purely software or cryptobased variant.

Self Help is also available as separate add-on.

Password rules
SafeGuard Easy offers a multitude of options for implementing special password rules in the PBA such as a configurable list of forbidden passwords, extended rules for special characters, UID etc., to provide even better functionality for implementing pre-defined corporate rules.

Auditing in the PBA and operating system
SafeGuard Easy also logs events involving security issues, such as failed logon attempts, in the Pre-Boot phase, and later passes on these log entries to the Windows Event Log for evaluation. Alternatively (via an additional component) they can be transferred to a central server, and evaluated there. As a result, attacks can be recognized more quickly and statuses diagnosed more easily.

Optional central administration database
In addition to its functions for reliably distributing configuration files, SafeGuard Easy includes a dedicated, central administration software system. This is responsible for system kernel backups, the distribution of configuration data and the integration of offline clients.

SafeGuard Easy uses a Microsoft Access or Microsoft SQL Server database as the default database type for saving information about SafeGuard Easy clients. With the "Remote Administration" module, which is also available, it is possible to configure a specific individual client over the network.

Same user password for SafeGuard Easy and Windows (password synchronization)
For many support staff, calls from users who have forgotten their password are part of everyday life. The rule is: the fewer passwords a user needs to remember, the less work there is for support staff. SafeGuard Easy's password functionality helps reduce the number of user calls because the software can be configured to make the Windows and SafeGuard Easy password the same ("synchronized") with just one mouse click. After successful synchronization, a user can then use the same password to log on to SafeGuard Easy in Pre-Boot Authentication and to the operating system.

Secure Wake-On-LAN support
SafeGuard Easy's Pre-Boot authentication offers the best-possible protection against attacks from hackers. However, maximum security is also needed when distributing software via Wake-On-LAN when active hard disk encryption is in operation, and so SafeGuard Easy offers a range of functions for that purpose.

Secure remote administration (Challenge/Response)
Helpdesk staff can help users who have forgotten their password. The Challenge/Response procedure is secure and ideal for mobile users, since it does not require a PC to have a direct online link with the help desk.

Challenge/response for PDA
SafeGuard Easy users who have forgotten their passwords or token can quickly return to work with help from a central help desk. Helpdesk staff can also carry out their work on an entirely mobile basis, using a PDA (Pocket PC), so they are no longer dependent on having access to a PC.

Windows Installer-based installation
As the installation procedure is fully compliant with the current Windows Installer (MSI) standard it can be distributed and installed easily and efficiently in Windows networks.

Integrated boot manager (Twinboot)
Today, it is a frequent requirement that a notebook's hard disk is split into a private, unprotected partition, managed by the user, and an encrypted partition that is managed by the user's company. SafeGuard Easy provides an integrated boot manager for this purpose, with which configurations of this kind, or similar ones, can be implemented easily and securely, from one central point. In this way the company data remains protected and the user has absolute freedom on their private partition, even when it comes to choosing the operating system.

Removable media encryption covers USB memory media
SafeGuard Easy supports the current generation of Plug and Play memory cards (USB memory sticks), so they can also be used for secure data exchange. In addition, it is possible to temporarily switch encryption for a particular diskette drive or removable media disk drive on or off, separately from the others.

Flexible user management during Pre-Boot Authentication
When a user is logging on, SafeGuard Easy can also add an additional message, specified by the administrator, that informs the user of legal requirements, ownership of the device, or similar.

Reusing configuration files from older versions (from SafeGuard Easy 3.20 onwards)
Companies use SafeGuard Easy's configuration files if a large number of clients are to use the same SafeGuard Easy configuration. In this situation the "old" configuration files can be imported to provide an easy way of reusing settings and keys during an upgrade without having to type them in again.

Emergency boot from diskette and CD
Nowadays, PC systems are usually equipped with CD/DVD drives instead of diskette drives. SafeGuard Easy has taken these hardware developments into account and now also accepts CDs as emergency boot devices, alongside floppies. Boot media are supported for both MS DOS and Windows PE.

Standard Windows logon instead of SafeGuard dialog
After SafeGuard Easy has been installed, you only see the Windows dialog when you log on to the operating system. However, customers can also customize the default logon and use a dialog that is based on the Utimaco design instead of the Windows logon dialog.

SafeGuard plug-in for Aladdin's Token Management System (TMS)
The Aladdin Token Management System (TMS) is a tool based on Active Directory and is used to issue eTokens. From version 1.1 the Aladdin TMS can be used to integrate plug-ins from third-party suppliers. In this way Utimaco has made it possible to use a plug-in to write SafeGuard Easy (PBA) data and SGAS Windows logon data can be to the eToken. The combination of TMS and Utimaco plug-in mean there is no need to use SafeGuard Token Administration to issue eTokens, but both programs can also be used in parallel. The SafeGuard TMS plug-in can be bought separately. A 10-user demo license is supplied with SafeGuard Easy (it can also be downloaded).

"Faster" user switch with token
Users who use SafeGuard's token-based logon also benefit from another feature: if it is necessary to change the SafeGuard Easy rights profile on a multi-user PC (for example, to switch off the right to encrypt removable media), the token users simply need to log off from Windows. There is no longer any need to reboot the PC completely or log on to PBA, as was previously the case.

NOTE: Do not confuse the SafeGuard Easy user switch with the Microsoft feature that has the same name!

Compatibility with Windows XP's Volume Shadow Copy service
Windows XP's Volume Shadow Copy service creates an "immediate backup" of opened files or databases. This means that there is no need for staff to stop working while an administrator saves their data. SafeGuard Easy provides full support for the Volume Shadow Copy service, so no changes have to be made manually to system configurations.

NOTE: as an alternative to the Windows XP copy function, users can also use other SafeGuard Easy-compatible tools such as Rescue and Recovery (which is also available for non-Lenovo platforms).

1.3 New features in SafeGuard Easy

Version 4.50 of SafeGuard Easy has resolved some problems identified in previous versions. For further details please refer to file `Readme.txt`.

New features in SafeGuard Easy 4.50

Support of the latest operating system service releases
The SafeGuard Easy Client has been tested to work with the latest version of its supporting platforms which include Windows XP Service Pack 3 as well as Windows Server 2003 Service Pack 2.

Support of latest token hardware and middleware
SafeGuard Easy has been updated to support the latest versions of Aladdin (CardOS) and RSA (SID800) hardware and middleware.

SafeGuard Easy also supports Aladdin NG-Flash USB token. The token can be used to authenticate the user in SafeGuard Easy Pre-Boot Authentication (PBA) and management applications in the same way as other tokens from Aladdin, VeriSign and RSA.

SafeGuard Easy 4.50 is compatible with the RSA data format SID800.

Optional installation of SafeGuard Easy Logging
The SafeGuard Easy Logging feature is no longer installed by default during the installation of SafeGuard Easy Client. This feature is now selectable as an optional feature in the main setup of SafeGuard Easy Client under Administration Tools.

Various minor improvements
Various minor improvements have been made, for example:

The setup will check for the operating system and will deny the installation in case of Windows Vista. With Windows Vista the preferred choice of a security solution would be to deploy SafeGuard Enterprise.

The tool RepPBA.exe will be delivered on the SafeGuard Easy product CD.This tool allows for changing the logon method within PBA, e.g. from logon with keyboard to logon with token.

You can find a complete list of all improvements in the file `Readme.txt`.

1.4 Changes to previous versions

Re-issuing a USB token
USB tokens that were issued with SafeGuard Easy **prior to version 4.11** cannot automatically be reused in the current version because the data format used on the token has been changed. These "old" tokens must be re-issued before you can log on to the PBA in the usual way.

In most cases, the user themselves is responsible for re-issuing the token (assuming that they have the appropriate SafeGuard Easy authorization). The first attempt to log on to the new version of SafeGuard Easy using the "old" token is met with the response "No SafeGuard Easy data on the token, please re-issue the token". However, people who are using "old" tokens should not be alarmed by this message: they should simply enter their SafeGuard Easy data in the pre-defined fields. If this data is correct it is written to the token and means that the only data they need the next time they log on is the token PIN.

If a user does not know their SafeGuard Easy data, they should get in touch with a support/help desk contact person. The contact person will then write the data to the token using the new SafeGuard Easy Plug-in for Token Administration.

The SafeGuard Easy Plug-in for Token Administration is stored in the \TOOLS directory (SCAdmin_SGEasy.msi) on the product CD.

SGEInteg replaces CheckArea/MigHelp
From Version 4.30, the repair function used when the SafeGuard Easy system kernel is updated is called "SGEInteg". SGEInteg provides the functionality previously provided by CheckArea/MigHelp. You will find it in the \TOOLS folder on the program CD.

1.5 System requirements

Supported operating systems (minimum)

- Windows 2000 Professional (Service Pack 4)
- Windows XP Home Edition (Service Pack 2)
- Windows XP Professional Edition (Service Pack 2)
- Windows 2000 Server (Standard Edition only)
- Windows Server 2003 (Standard Edition only)

Current Service Packs are recommended.

SafeGuard Easy has not been tested with Windows XP Media Edition.

Note concerning Windows XP
SafeGuard Easy versions 4.50 can be also used under Windows XP SP2 or SP3. It is also possible to upgrade from e.g. SP2 to SP3 while SafeGuard Easy is installed.

Note about Windows XP SP 2/Windows Server 2003 SP 1
If you use the optional central administration server or SafeGuard Easy 4.x Remote Administration you must make a few special configuration settings in Windows XP in SP2 and Windows Server 2003 SP 1.

You will find a description of all the settings you need in our Knowledge Database **http://www.utimaco.com/myutimaco** in Knowledge Item "106898 SafeGuard Easy and SP2 Configuration for Windows XP". Use the Knowledge Database's "Search" field to look for "106898".

An application with which you can set the configuration settings automatically has also been provided. This enables Central Administration and Remote Administration to be used with Windows XP Service Pack 2. You will find this application on the CD, in the \Tools\DCOMWizard folder, or in the Knowledge Database: look for it with the keywords "SP2" or "SGE".

Note about Windows XP Home Edition:
SafeGuard Easy does not support

- Secure automatic Logon with Smartcard (Smartcard-SAL)
- Centralized Auditing (Logging)

Note about Windows Server Edition:
SafeGuard Easy does not support

- SMP
- 64-bit server

Supported file systems

- FAT-12
- FAT-16
- FAT-32
- HPFS
- NTFS
- NTFS5

Supported memory media

- Hard disks (IDE, SCSI, serial ATA, Firewire, USB)
- Floppies
- Removable media such as ZIP/JAZ
- USB memory sticks
- RAID 0 (Hardware-RAID 0)

  SafeGuard Easy does not support:
  - additional RAID classes)
  - Software-RAID 0

Supported processors

- AMD
- Intel
- Multi-processors/hyperthreading
  SafeGuard Easy 4.x has been installed and tested successfully on both multi-processor computers and computers with hyperthreading (e.g. Pentium IV).

Hardware requirements

- **Hard disk capacity**
  SafeGuard Easy requires between 5 MB (minimum) and 15 MB (maximum) depending on the selected installation method. SafeGuard Easy has the same minimum requirements as the operating system currently in use.

  Although SafeGuard Easy runs smoothly and without any problems on the systems described, encryption comes at a cost. For this reason we recommend that you use hardware that exceeds these minimum requirements.

- **Number of hard disks**
  SafeGuard Easy supports a maximum of 4 hard disks per machine, with a maximum of 8 partitions per hard disk. The system displays a warning if an unsupported partition type is found.

1.6 Documentation

SafeGuard Easy is supplied with this manual and the SGEasy0409.chm online help file.

1.7 General notes

In normal operation, the following points should be taken into account:

- SafeGuard Easy does not support Windows XP's "Fast User Switching". After SafeGuard Easy has been installed, the Welcome screen switches off automatically.
- If the workstation is integrated in a peer-to-peer LAN, parts of hard disks must not be assigned to other users of this LAN.
- Hard disk drive encryption and decryption are protected against power cuts and similar disruptions. As soon as the power is restored, the process continues from the correct place without any need for a user action.

NOTE:
The initial encryption of hot-pluggable hard disks must not be interrupted!

- When you leave the workstation for a short time, you should enable Windows screen-blanking ([Lock workstation] button). If you want to leave the workstation for a longer period of time, switch off the PC and then switch it on, and reboot it, when you return.
- By correctly setting the recommended installation system configuration, you prevent logical access to hard disks after booting from diskettes. To give the system with additional protection against trojan viruses that might be used to find out a SafeGuard Easy password, use a mechanical lock or another internal measure to protect the workstation from being booted from diskette.

1.8 License note

All cases of unauthorized duplication of this manual or the software supplied by SafeGuard Easy will be pursued in law. You can only install SafeGuard Easy on one PC.

If you misuse the backup copy to install SafeGuard Easy on several PCs, you will contravene the terms of the license and be liable to punishment. If you want to protect several PCs you must purchase a license for each PC.

The terms and conditions of the software license contract apply.

Other license notes:
STEALTH Encryption Copyright (c) 1994 Intelligence Quotient International Limited. All rights reserved. Patents pending. STEALTH encryption is a trade mark of Intelligence Quotient International Limited.

Patent rights of Ascom Tech Ltd. given in EP, JP, US. IDEA is a trademark of Ascom, Tech Ltd.

Credits:
Special thanks go to Dr. Brian Gladman, whose AES implementation we used as the basis for building our AES encryption drivers.

2 Getting started

This chapter explains how to prepare for, and perform, your SafeGuard Easy installation successfully.

2.1 Preparing for installation

You must make some preparations prior to installation: please read the following list carefully and ensure that you comply with all the points.

- Before installing SafeGuard Easy please make a complete back up of your data media.
- All the hard disks that are to be encrypted must already be connected to the PC and switched on before SafeGuard Easy is installed.
- The partitions on your hard disk should be completely formatted and should have a drive letter assigned to them.
- Removable media or USB memory sticks that are to be encrypted do not have to be connected to the PC before SafeGuard Easy is installed.
- Use CHKDSK to check the hard disks for errors.

  You will find more information on this subject in the Utimaco Knowledge Database **http://www.utimaco.com/myutimaco**.

  Use the Knowledge Database's "Search" field to look for key words like "NTFS" or "File System".
- Virus scanners should be switched off during installation/ uninstallation.
- If you use a boot manager, consider reinstalling the system without the boot manager.

- If you used a clone tool (Drive Image Ghost) to write data to the hard disk, we recommend that you "re-write" the MBR.
  To install SafeGuard Easy you need a "spotless" master boot record. The use of Image/Clone programs may have affected the state of this record.

  You should clean the master boot record by booting from floppy, CD or DVD (we recommend you use the same system that is used on the hard disk) and run fdisk /MBR.

- If the boot partition has been converted from FAT to NTFS, and the system has not been reset by rebooting, SafeGuard Easy should not be installed. In this case it may be that the installation will not be completed because the file system was still FAT at the time of installation while NTFS was found when it was activated. In this case you have to reboot the machine once before SafeGuard Easy is installed.

SafeGuard Easy is undergoing constant further development. This means that your version may contain new features which were not included in the manual or online help because they were not ready in time for publication deadlines. These new changes or features are described in the `Readme.txt` file.

2.2 Installation prerequisites

Various prerequisites must be fulfilled on a workstation before SafeGuard Easy can be installed:

- **Microsoft Windows Software Installer (MSI) v2.0**
  - Installed by default in Windows XP.
  - Installed in Windows 2000 from Service Pack 3 onwards.

- **High Encryption package (only necessary for Central Administration with SafeGuard Easy Database)**
  The Central Administration system, using the SafeGuard Easy Database and SafeGuard Easy Server, requires that Windows supports encryption with 128-bit keys.
  - Installed by default in Windows XP
  - Installed in Windows 2000 from Service Pack 2 onwards.

2.3 Installable modules

SafeGuard Easy consists of different "modules" that work independently of each other.

The different modules are MSI packages which are stored on the product CD in the SGEASY\INSTALL folder in the CLIENT, SERVER and RUNTIME folders. You will find the files you need in the sub-folders, sorted by language.

These modules are available:

`SGEasy.msi`	Client Application for SafeGuard Easy
`Runtime.msi`	Runtime system
`Server.msi`	SafeGuard Easy Server

SafeGuard Easy, the runtime system, and the SafeGuard Easy Server, are installed as different products. As a result, they also appear separately in the list of software present on a system.

2.4 User interface language

If you start the installation via "setup.exe", the user interface language used during and after the installation of SafeGuard Easy is the one set using the Regional Options in the Control Panel. SafeGuard Easy supports German, English and French. If, for example, "German" is the current Regional Option, the user interface is displayed in German. The same applies for "English (United States)" and "French".

The online help is always available in whatever language you selected during installation. If you change the Regional Options you do not change the language in which the online help is displayed.

If you start the installation via an msi file, the user interface language is always English. To support other languages (French/German) you must perform a number of "transforms". The Windows Installer uses transform files to automatically toggle the installation package to the new language. The following transform files are currently available:

`Sgeasy_f.mst` (for French) and `Sgeasy_g.mst` (for German).

To change the language in which text appears during installation, run this command before installation:

`msiexec /I` <MSI package> `TRANSFORMS=`<transform file>

For example, for a German-language installation you must execute this command line:

```
msiexec /I Sgeasy.msi TRANSFORMS=Sgeasy_g.mst
```

Note that the TRANSFORMS parameter must always be written in capital letters!

To simplify installation you can use the `setup.exe` file which automatically selects the set language for the Installation Wizard and runs `SGEasy.msi`. `SGEasy.msi` uses the `Setup.ini` file in which additional parameters can be defined, provided they are entered using the syntax `CmdLine=` {Parameter1, Parameter2,..}.

The same applies for the installation of the runtime system (`Runtime.msi`) and the SafeGuard Easy Server (`SGEasy.msi`).

3 Local installation

In a local installation, SafeGuard Easy is installed on a single stand-alone client from the product CD. To perform a local installation, follow these steps.

The user who is to install SafeGuard Easy must be logged on with **Windows Administrator rights**, as it will be necessary to access the hard disk, and install drivers and system services that also require administrator rights.

3.1 Step by step

How to install SafeGuard Easy:

1. If you use a program CD, installation starts automatically after you insert the CD in the CD-ROM drive. (If it does not, run the `Setup.exe` file in the \CLIENT folder on the program CD). An Installation Wizard then leads you through the installation. Click [Next].

2. The *License Agreement* dialog is displayed. If you agree to the license terms, select the "I accept the license agreement" check box. If you do not agree to the license terms, the installation ends. Click [Next].

3. The *Target Folder* dialog is displayed. Enter the required target folder. The standard installation folder is \UTIMACO\SafeGuard on the boot drive. If a SafeGuard product is already present on the workstation, its installation folder is selected automatically.
   Do not enter special characters in the folder name!
   Click [Next].

4. In the *Select Installation Type* dialog, select which features are to be installed. Select the features you require. Then click [Next].

   Encryption
   installs SafeGuard Easy complete with all its available features. The only optional ones are:

   - **Secure Auto Logon (SAL)**
     Remembers the Windows access data used in initial logon so that only the SafeGuard Easy user data needs to be entered in Pre-Boot Authentication to log on (see 'Secure Automatic Logon (SAL)').

- **Server connection (network agent)**
  This is essential for encrypted communication between the client and server, if the workstation is to be administered centrally. The network agent does not need to be installed if the workstation is only to be used as a stand-alone device (see 'Central administration').

- **Smartcard Auto Logon**
  Automatically transfers the Windows access data to a smartcard so that only the SafeGuard Easy user data needs to be entered in Pre-Boot Authentication for logon (see 'Secure Automatic Logon with smartcard (Smartcard SAL)').

- **FIPS Mode**
  Guarantees that SafeGuard Easy runs in accordance with FIPS 140-2 Level 1 (see 'FIPS 140-2 (Level 1) certification').

Administration tools

You do not need to install all the product features on an administrator workstation that will only be used to administer SafeGuard Easy clients. Usually you only need the administration tools (warning: SafeGuard Easy Administration is not installed with administration tools). The administration tools include

- **SafeGuard Easy Logging (Auditing)**
  Used for auditing security related log events triggered by installed SafeGuard products. In addition to pure logging this feature also includes a filter mechanism that supports the administrator in selecting the relevant events (see 'Auditing').

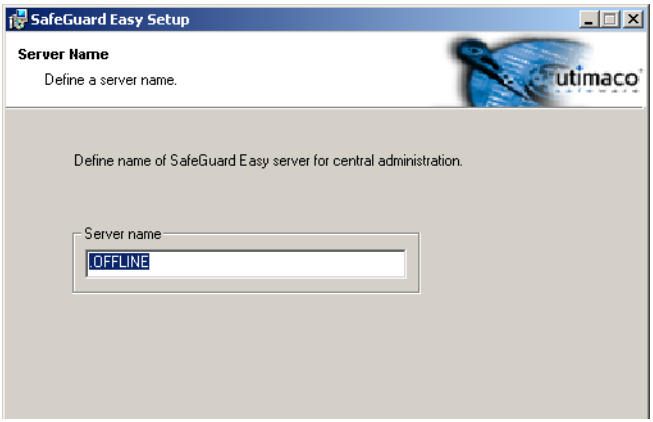
- **Configuration File Wizard**
  Generates files that update the current configuration of a client once they have been run, for example by adding a new user (see 'Configuration File Wizard').

- **Response Code Wizard**
  Used to permit users to perform specific actions (for example, set new password), even if the administrator is not present (see 'Remote maintenance (Challenge/Response)').

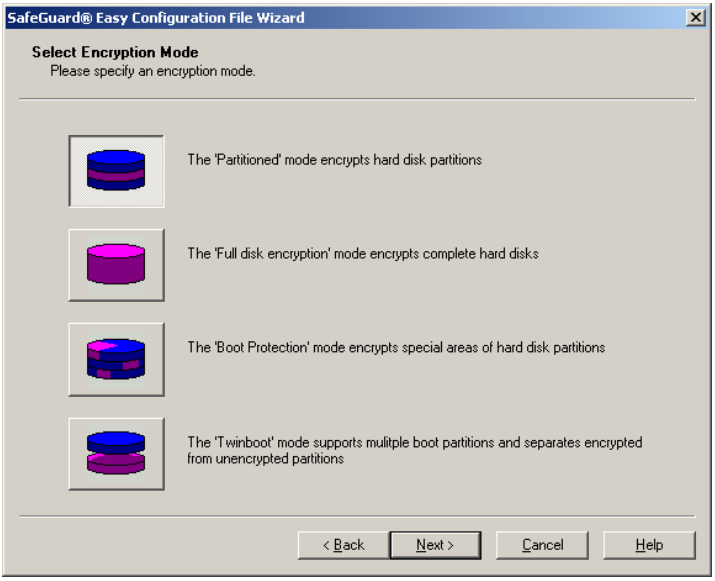
- **Administration Token Support**
  Permits token-based logon to SafeGuard administration tools, including Administration (see 'Secure Automatic Logon (SAL)').

You will find more detailed information about the installation options in the relevant chapters.

5. If "Server Connection" was selected, enter the name of the SafeGuard Easy Server.



6. Next, select the **encryption mode** for the hard disks on your PC. You will find a detailed description of this under 'Encryption mode'.


SafeGuard® Easy Configuration File Wizard
Select Encryption Mode
Please specify an encryption mode.
The 'Partitioned' mode encrypts hard disk partitions
The 'Full disk encryption' mode encrypts complete hard disks
The 'Boot Protection' mode encrypts special areas of hard disk partitions
The 'Twinboot' mode supports mulitple boot partitions and separates encrypted from unencrypted partitions
< Back
Next >
Cancel
Help

7. In the next step you make the specific configuration settings. You will find a detailed description of the settings in the relevant chapters in the manual.

NOTE:
The "with token only" setting (see General / Authentication / Logon) means that SafeGuard Easy requires token-based logon for **all** SafeGuard Easy users on a workstation.

If the "with token only" method is selected, a user can only log on in PBA if the token already contains valid SafeGuard Easy data. If the token is blank you cannot log on in PBA.

8. In the next step you are prompted to enter passwords for the pre-defined SafeGuard Easy user profiles SYSTEM and user. These passwords must correspond to the SafeGuard Easy password rules.

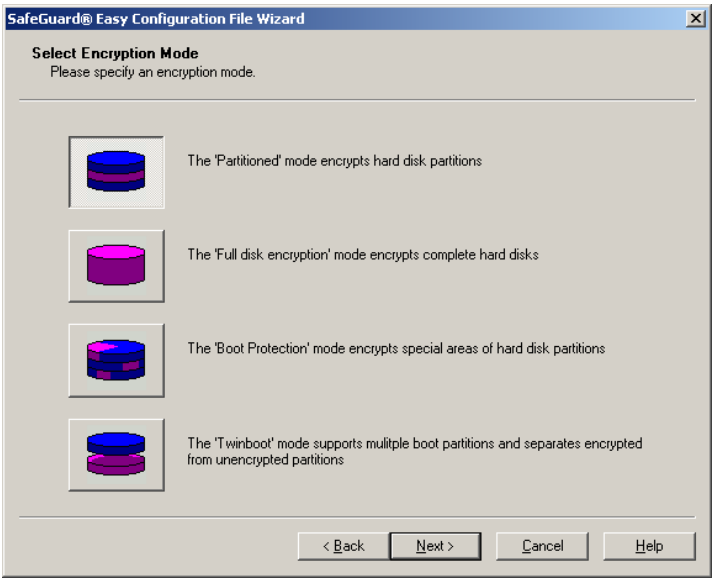
NOTE:
Please remember the passwords that are entered here. If the "Password at system start" (= Pre-Boot authentication) option in the General folder is enabled, you can only log on to your workstation with these user names and passwords!

9. The installation is now finished.

10. Reboot the PC.

3.1.1 Encryption mode

Encryption mode must be specified if SafeGuard Easy is installed interactively or within a configuration file that has the "Install" attribute.


SafeGuard® Easy Configuration File Wizard
Select Encryption Mode
Please specify an encryption mode.
The 'Partitioned' mode encrypts hard disk partitions
The 'Full disk encryption' mode encrypts complete hard disks
The 'Boot Protection' mode encrypts special areas of hard disk partitions
The 'Twinboot' mode supports mulitple boot partitions and separates encrypted from unencrypted partitions
< Back
Next >
Cancel
Help

- **Partitioned**
  In this mode, SafeGuard Easy only applies the encryption to individual partitions. You should select this setting if your hard disk drive(s) has/have several partitions and you do not want to encrypt all of them. In the Encryption settings you decide which partitions you want to encrypt.

- **Full disk encryption**
  All hard disks connected to your workstation are completely encrypted. SafeGuard Easy automatically recognizes whether your computer has one or more hard disk drives. The program can be installed under Windows on systems with up to four physical hard disk drives. If more than four hard disks are identified, SafeGuard Easy discontinues the installation procedure. Up to eight logical partitions can be present on each of these hard disks.

- **Boot Protection**
  Boot protection ensures is that no-one without the appropriate authorization can boot the computer from a system floppy disk/CD/DVD to access the computer's hard disk. Boot protection is only effective when combined with activated Pre-Boot Authentication (see 'Switching on password at system start (PBA)').

  Boot Protection completely encrypts partitions that are not formatted or that it cannot identify.
  In the case of FAT and FAT32 the system areas are encrypted.
  In the case of NTFS, the partition is encrypted from the start of the partition to the end of the MFT (Master File Table).

- **Twinboot (available with two primary partitions only)**
  If you select this option, two partitions are generated. One is encrypted, and one is unencrypted. Both must be bootable primary partitions. If the PC is booted from the encrypted partition, there is no way of accessing the unencrypted partition, and vice versa. In this way private data can be kept quite separate from commercial data.

  If the PC is booted from the encrypted partition, the user must enter the SafeGuard Easy password for PBA. There is no SafeGuard Easy password protection for the unencrypted partition.

  You will find details about the Twinboot procedure in chapter 'Twinboot/Boot Manager'.

3.2 After installation

Reboot the workstation
After the installing (or removing) SafeGuard Easy, the workstation must be shut down and restarted. Any applications open at this point in time are also closed without being saved. To avoid losing your data, we strongly recommend that you close all active applications before installation/ deinstallation.

PBA appears after the second reboot
After the first reboot, PBA is inactive. At this time a Windows user only has *AUTOUSER rights. As soon as a Windows user logs on and shuts down the workstation, the PBA logon screen appears (if PBA is switched on) and a SafeGuard Easy user can log on to the system.

System start from floppy
If the system has not yet finished encrypting the hard disk when a session is ended, the computer ALWAYS reboots directly from the hard disk, i.e. it is not possible to boot from a system floppy disk. This also applies for the first restart after encryption has completed.

Do not change the partitioning on the hard disk
If the first hard disk drive (or a partition) was encrypted, do not add or remove partitions! To reorganize the first hard disk drive, uninstall SafeGuard Easy (=decrypt the first hard disk drive), create/remove partitions and re-install SafeGuard Easy again.

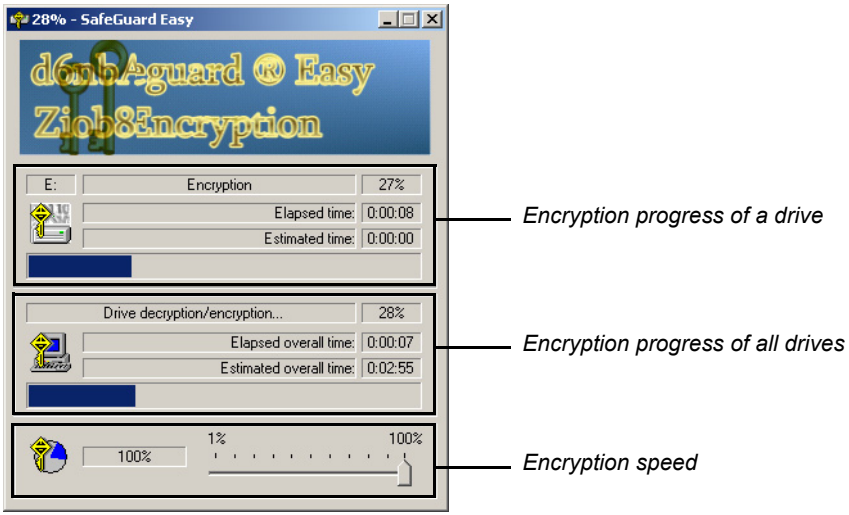
Do not interrupt the initial encryption of "Hot-Pluggable" drives
"Hot-pluggable" is the term used to describe USB devices that can be connected and disconnected without the need to reboot the computer. You must not interrupt the initial encryption of hot-pluggable hard disks.

Initial encryption
Allow between 20 and 30 minutes for SG Easy to perform initial encryption on 10 GB of data, with AES-256, on a modern notebook.

If, for any reason the initial encryption fails and the computer cannot be booted anymore, please contact Utimaco’s support team.

3.3 Displaying encryption progress

If hard disk or partition encryption was activated during installation, the Encryption Status screen is displayed: it shows the encryption progress.



The encryption procedure runs entirely in the background, i.e. the user can continue working at their computer throughout the encryption process. If very small partitions are being encrypted, or only the system area, the screen may not be displayed.

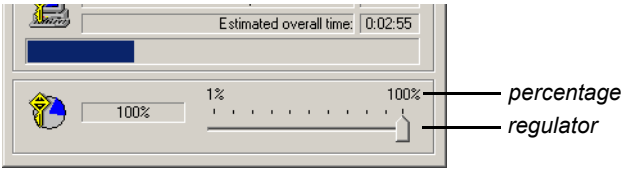
3.3.1 Switching off the status screen

SafeGuard Easy can suppress the encryption status screen. To do so, you must enter a new registry key [DWORD]:

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy
ShowECView"=0

3.3.2 Defining encryption speed

The default setting for the encryption speed is 100%, but you can use the regulator to adjust this. The higher the selected percentage, the faster encryption takes place.



If you use the regulator to reduce the encryption speed, SafeGuard Easy does not save the reduced encryption speed. After the workstation is rebooted, encryption starts again at full speed (100%).

Setting a default encryption speed value

The speed value for the encryption process can be adjusted. Every time the system boots, the encryption speed is set to that value. To do this, enter a new registry key [DWORD]:

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy
"**DefaultCPUUsage**"=<percentage>

If the registry key is present, the encryption process resumes after a restart with the percentage value you specified. However, you can use the regulator to increase or decrease this percentage value.

Setting a maximum encryption speed value

The default maximum encryption speed (100%) can be reduced. To do this, enter a new registry key [DWORD] and enter a percentage value (for example "75"):

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy
“MaxCPUUsage”=<percentage>

Deactivating the regulator

To prevent users from changing or affecting the speed of the encryption process, you can also **deactivate the regulator** by generating the [DWORD] registry key

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SgEasy
"ChangeCPUUsage"

and setting the value to "0".

The regulator then appears grayed out.

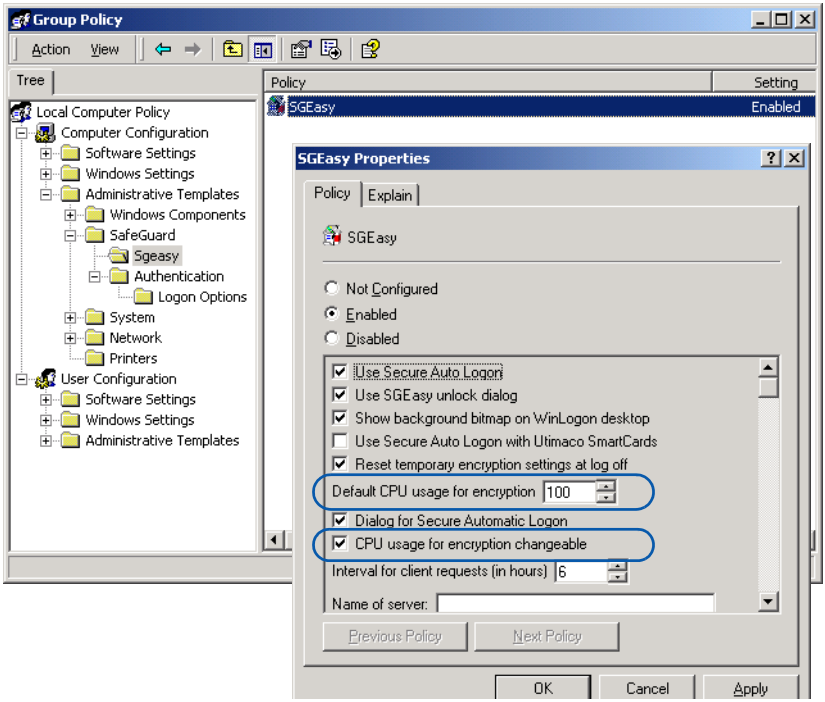
Changing encryption speed settings in the administrative template

The CPU settings can also be switched on or off via a policy in Utimaco’s administrative template (’Changing frequently-used Registry settings with SafeGuard Easy’s administrative template’).

You will find this policy in

Computer configuration
\Administrative templates
\SafeGuard
\SGEasy

On the Properties tab of the "SGEasy" policy the "Default CPU usage for encryption" and "CPU usage for encryption changeable" options are provided for this purpose.



3.4 Changing the background bitmap in the Windows logon dialog

You can choose a different bitmap for the system to display when the user enters their SafeGuard Easy user data. This allows customers to modify the background displayed for SafeGuard Easy to meet their company's own requirements.

The default background bitmap displayed is called **SgeLogo.bmp** and is stored in the selected **SafeGuard Easy folder**.

To swap the title bitmap, simply replace the default bitmap with a modified bitmap with the same name and size.

If you **do not want ANY background bitmap** to be displayed, set the

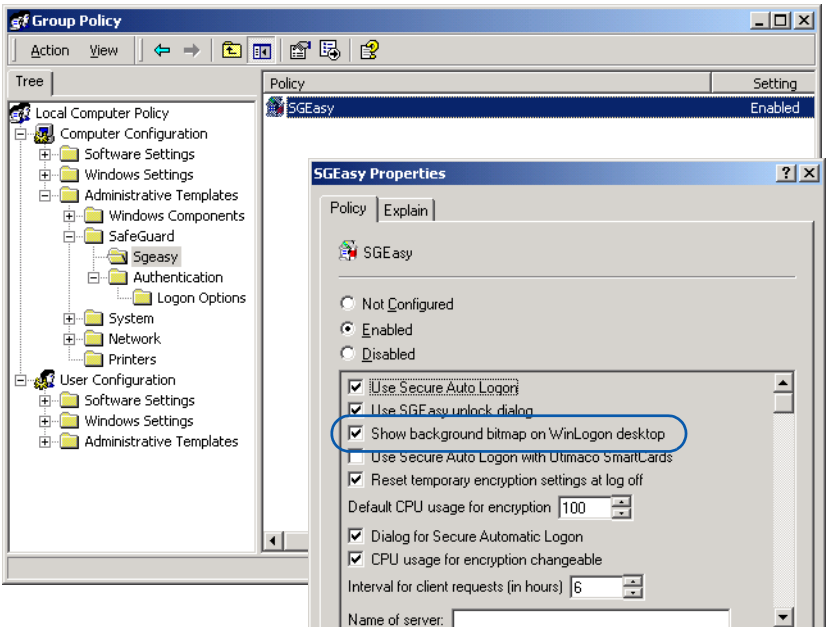
HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SgEasy
SgeLogoBackGnd
registry key to "0"

The size of the title bitmap is 640x480 pixels and it has a maximum color depth of 8 bits.

You can also switch off the background bitmap via Utimaco's administrative template. You will find the policy in

Computer configuration
\Administrative Templates
 \SafeGuard
  \Sgeasy

On the "SGEasy" property page deselect the "Show background image on Winlogon Desktop" option and the SafeGuard Easy bitmap will no longer appear.



3.5 Installing SafeGuard Easy on a PC with multiple operating systems

SafeGuard Easy can be installed on a computer to protect the data on it, even if several operating systems are installed in separate partitions on the computer. To ensure that the operating systems can also be booted correctly after SafeGuard Easy has been installed, you must perform a full installation of SafeGuard Easy on one of the operating systems and, on each of the other operating systems, install what is known as the "runtime system".

You run the Runtime System MSI package, `Runtime.msi`, from the \RUNTIME folder on the CD. A runtime system also installs SGECRYPT, the program for toggling floppy disk drive and device encryption.

How to install SafeGuard Easy on a PC with multiple operating systems:

1. Select one Windows installation as the primary installation.

2. Now boot all non-primary Windows installations, in sequence, and install the runtime system on each of them. For each installation, select a different folder.

3. Finally, boot your primary Windows installation and then install SafeGuard Easy.

4. After encryption is complete you can then also boot all the non-primary Windows installations.

4 Central installation

Administrators can set up the entire configuration for user PCs as part of central software distribution.

To do so, an Administrator creates a file on their PC that contains the all necessary SafeGuard Easy settings for the user PCs. SafeGuard Easy calls this file a "configuration file". This configuration file is used to install SafeGuard Easy on the user PCs. You can always make changes to the SafeGuard Easy configuration later via other configuration files.

SafeGuard Easy can be installed in an environment in which Active Directory is also installed, or not.

4.1 Creating the configuration file

How to create a configuration file:

1. Call the Configuration File Wizard via **Programs/Utimaco/SafeGuard Easy/Configuration file wizard**.

2. To install SafeGuard Easy, select the "Install" property for the configuration file. The configuration file is generated once all the required settings and entries have been made in the individual admin pages in the configuration program.

3. When the configuration file is generated, a file is created, which is called `Install.cfg` by default in the case of an installation.

This .cfg file contains all the details of the required configuration on the target computer. It is encrypted and contains the keys (for the hard disks/ floppy disk drives/removable media) and the passwords for the users.

For more details see 'Configuration File Wizard'.

> ***NOTE:***
> Configuration files must be protected from unauthorized access. Regular users must not access configurations files.

4.2 Installation with Active Directory

You install SafeGuard Easy on clients in an Active Directory environment by adding a (modified) MSI package (`SGEasy.msi`) to the software distribution function of a group policy object (GPO).

To modify the MSI file you need an editor that can edit MSI files (for example, ORCA or NetInstall). ORCA is provided in the Microsoft Windows Installer Software Development Kit (SDK).

4.2.1 Prerequisites

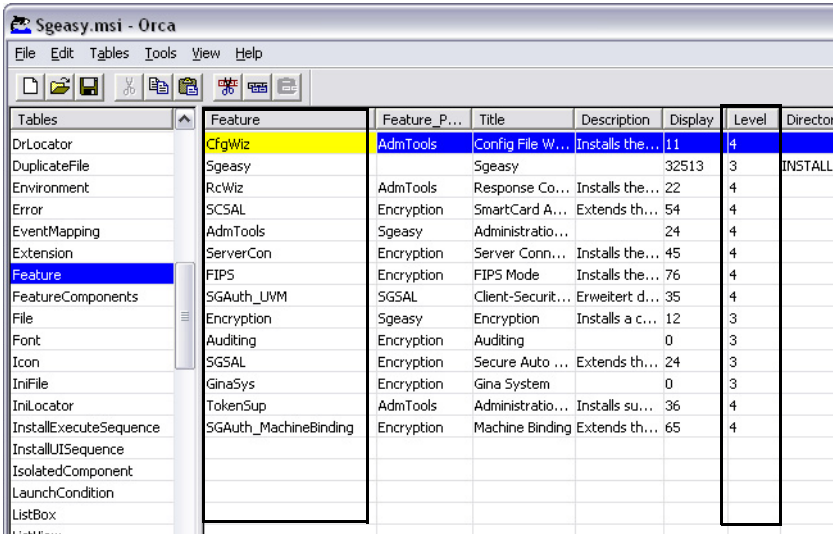
- You must ensure that either Windows 2000 or Windows XP is running on the user PCs.
- All the devices on which installation is to be performed must first have been added to the organizational unit for which the configured GPO (group policy object) is used.
- Client PCs are assigned to the directory domain for central software distribution, and a computer account has been set up and is active for each PC.
- There is enough disk space available on the system partition.

4.2.2 Using an editor to modify MSI files

If, for example, you are working with ORCA, you must specify which SafeGuard Easy "Features" are to be installed. To do this, change the value in the "Level" column.

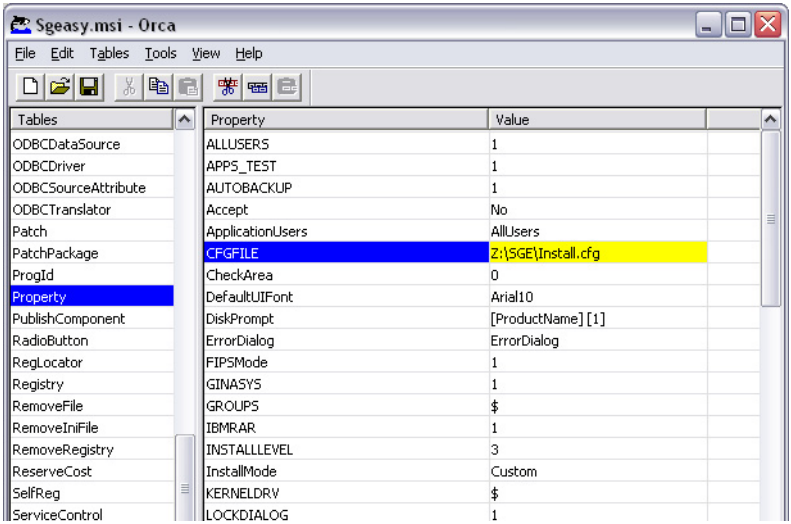
3 = Feature will be installed.
4 = Feature will not be installed.

You will find a detailed description of all the features at 'SafeGuard Easy features'.


Sgeasy.msi - Orca
File Edit Tables Tools View Help
Tables
DrLocator
DuplicateFile
Environment
Error
EventMapping
Extension
Feature
FeatureComponents
File
Font
Icon
IniFile
IniLocator
InstallExecuteSequence
InstallUISequence
IsolatedComponent
LaunchCondition
ListBox
Feature | Feature_P... | Title | Description | Display | Level | Director
CfgWiz | AdmTools | Config File W... | Installs the... | 11 | 4
Sgeasy | | Sgeasy | | 32513 | 3 | INSTALL
RcWiz | AdmTools | Response Co... | Installs the... | 22 | 4
SCSAL | Encryption | SmartCard A... | Extends th... | 54 | 4
AdmTools | Sgeasy | Administratio... | | 24 | 4
ServerCon | Encryption | Server Conn... | Installs the... | 45 | 4
FIPS | Encryption | FIPS Mode | Installs the... | 76 | 4
SGAuth_UVM | SGSAL | Client-Securit... | Erweitert d... | 35 | 4
Encryption | Sgeasy | Encryption | Installs a c... | 12 | 3
Auditing | Encryption | Auditing | | 0 | 3
SGSAL | Encryption | Secure Auto ... | Extends th... | 24 | 3
GinaSys | Encryption | Gina System | | 0 | 3
TokenSup | AdmTools | Administratio... | Installs su... | 36 | 4
SGAuth_MachineBinding | Encryption | Machine Binding | Extends th... | 65 | 4

NOTE:
If you want to install a feature you must also install its “Feature Parent”.

The "Property" table section lists the SafeGuard Easy parameters. In the SafeGuard Easy "CFGFILE" parameter, for example, you enter the location of the configuration file.



You will find a detailed description of all parameters in 'SafeGuard Easy setup parameters'.

Please refer to the appropriate Microsoft documentation to learn more about modifying msi files with ORCA.

4.2.3 Deploying MSI files

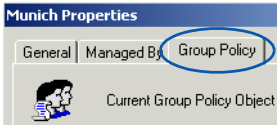
To do this:

1. Share a local drive on the Administrator's PC (remove the write-protection) and copy all the required .msi files to this drive. Ensure that the clients can access the shared drive!

2. In Windows, click **Start/Settings/Control Panel/Administrative Tools**. There, select **Active Directory users and computers**.

3. Right-click a domain or organizational unit and select *Properties*.

4. Select the Group Policy tab in the *Properties* dialog.



5. Create a new group policy object (e.g. "GPO installation") by clicking the [New] button.

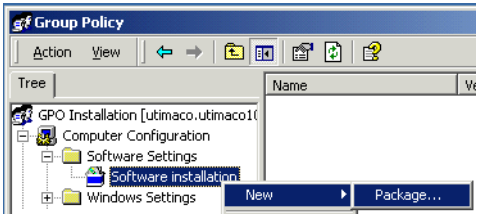
6. Click the [Edit] button.

7. Windows displays the "GPO installation" group policy.

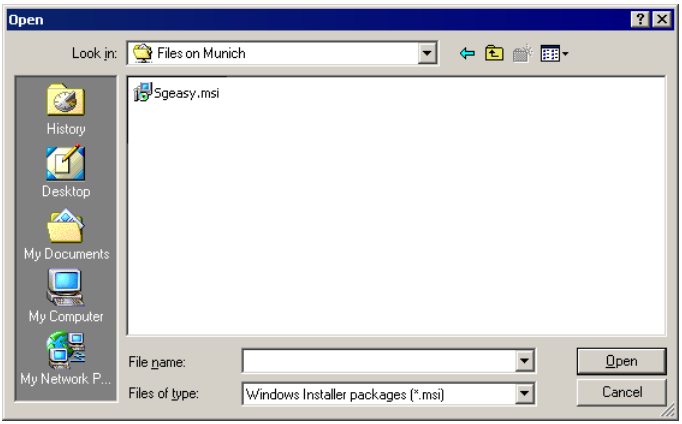
8. Select **Computer Configuration/Software Settings/Software Installation**. In the Software Installation's context menu, create a link to the file server that will deploy the software packages.

NOTE:
Only add msi packages to the Software installation of the **Computer Configuration**. Installations via User Configuration are not supported.

9. Right-click *Software installation* and then select *New* and *Package*.



10. Select one (or more) .msi files from the shared directory. Load the files from the real network path (UNC path)!



11. When you have confirmed all the prompts, Windows adds the .msi file to the group policy object's installation routine.

12. Close the dialog.

13. If you want the operating system language to be ignored on the client side, open the context menu of the installed Msi package and select Properties/Deployment/Advanced/Ignore language when deploying that package.

The "GPO installation" group policy object will now be used on all computers/users present within the domains of an organizational unit. The next time these workstations are rebooted, the packages will be installed there unattended.

Before rebooting the connected PCs, please check, if

- the PCs designated for installation have also been added to the organizational unit for which the GPO is configured.
- the clients are attached to the folder domain to perform central software distribution. In addition, an active computer account for the client PCs must be created on the domain.
- there is enough space available on the system partition.

4.3 Installation without Active Directory

To install SafeGuard Easy without an Active Directory environment you need software distribution programs from third-party suppliers.

In this case, create an installation package that contains

- the SafeGuard Easy program files
- a script with the command line for the preconfigured installation

Distribute the installation package to the clients.

4.3.1 Command line syntax for unattended installation

If you to install SafeGuard Easy without Active Directory, use the MSIEXEC program. MSIEXEC comes as standard with Windows 2000 and Windows XP. If the system administrator creates configuration files, this installation program is used to run them automatically. In this program the system administrator can specify both the source and target for installation, so that a uniform installation can be performed on a number of PCs.

Command line syntax

`msiexec /i` <path+msi Package Name> `/qn ADDLOCAL=ALL |` <features> <SGEasy parameters+configuration file>

The command line syntax contains the following information:

- **parameters used by Windows Installer** that, for example, log warnings and error messages in a file during installation.
- **SafeGuard Easy features** that are to be installed with a SafeGuard Easy packet (for example, Response Code Wizard).
- **SafeGuard Easy's own parameters**, used, for example, to specify which configuration files are to be used.
- **a configuration file,** for an installation with the "Install" property.

Example:

```
msiexec /i F:\Sgeasy.msi /qn /L* I:\Temp\SGE.log
ADDLOCAL=Sgeasy,Encryption,SGSAL
Installdir=C:\SGE CFGFILE=F:\Install.cfg
```

SafeGuard Easy is installed with SAL in the installation folder, C:\SGE, and the log file SGE.log is created in the I:\Temp folder (which must already be present). The preconfigured settings for SafeGuard Easy are stored in the `Install.cfg` configuration file.

List the individual features, separated only by a comma, with no additional blank spaces. Ensure you spell the names of individual features using the correct upper and lower case letters.

If you select a feature you must also add all the parent features to the command line!

4.3.2 Selected options used by Windows Installer

> ***NOTE:***
> Run msiexec.exe from the Windows command prompt. The system then displays all available Windows Installer options.

`/i`
Shows that an installation is involved.

`/qn`
Installs without user interaction and does not display a user interface.

`ADDLOCAL=`
Lists the features that are to be installed. If this parameter is not specified, all the features that form part of a Full disk encryption installation are installed.

`ALL`
Installs all available features.

`REBOOT=Forcerestart | NORESTART`
Forces or prevents restart after installation. If you do not specify a value, restart is forced after installation (default = Force).

`/L*` <path + file name>
Logs all warnings and error messages in the specified log file. To only log error messages, enter the parameter `/Le <path + file name>`.

`Installdir= <folder>`
Specifies the folder in which SafeGuard Easy is installed. If you do not specify a value, the default installation folder is used: <SYSTEM>:\Program Files\UTIMACO.

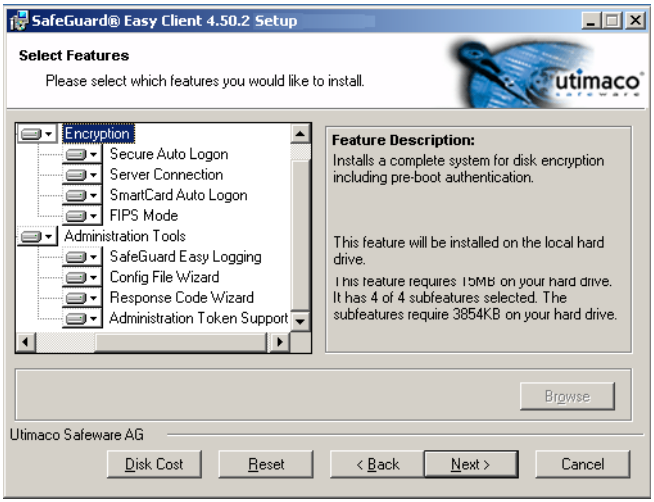
4.4 SafeGuard Easy features and parameters

To perform a central installation you must make a few advance preparations. You must specify which SafeGuard Easy features/ parameters are to be installed on the clients. To install SafeGuard Easy in an Active Directory environment you can, for example, use the ORCA tool to modify the MSI file. Without Active Directory, the features must be listed in the command line.

4.4.1 SafeGuard Easy features

The following tables show all the SafeGuard Easy features that can be installed automatically with one of SafeGuard Easy's .msi files. They are exactly the same as the features that can be selected during an interactive installation.

In the example, you see all the Sgeasy.msi features that can be selected during a Custom interactive installation.


SafeGuard® Easy Client 4.50.2 Setup
Select Features
Please select which features you would like to install.
utimaco
Encryption
Secure Auto Logon
Server Connection
SmartCard Auto Logon
FIPS Mode
Administration Tools
SafeGuard Easy Logging
Config File Wizard
Response Code Wizard
Administration Token Support
Feature Description:
Installs a complete system for disk encryption including pre-boot authentication.
This feature will be installed on the local hard drive.
This feature requires 15MB on your hard drive. It has 4 of 4 subfeatures selected. The subfeatures require 3854KB on your hard drive.
Browse
Utimaco Safeware AG
Disk Cost
Reset
< Back
Next >
Cancel

Features that can be installed with SGEasy.msi		
Feature	**Feature Parent**	**Description**
Sgeasy	---	Installs all the files required for using SafeGuard Easy. No features are active after an automatic restart. They can be activated at any time without user interaction (or manually via Control Panel/Add/Remove Programs).
Encryption	Sgeasy	Installs a working SafeGuard Easy (incl. SafeGuard GINA).
SGSAL	Encryption	Installs the SAL
ServerCon	Encryption	Installs the Server connection (network agent) for Central Administration
SCSAL	Encryption	Installs the SAL with Smartcard
FIPS	Encryption	Installs FIPS mode
AdmTools	Sgeasy	Installs the administration tools (e.g.Configuration File Wizard, Response Code Wizard) No features are active after an automatic restart, but they can be activated at any time either without user interaction (or manually via Control Panel/Add/Remove Programs).

Features that can be installed with SGEasy.msi		
Auditing	AdmTools	Installs SafeGuard Easy Logging.
CfgWiz	AdmTools	Installs the Configuration File Wizard.
RcWiz	AdmTools	Installs the Response Code Wizard.
TokenSup	AdmTools	Installs token-based logon to the administration tools.
SGAuth_UVM	SGSAL	Extends the Windows Logon Procedure by supporting the ThinkVantage Client Security Integration Features.
SGAuth_Machine Binding	Encryption	Extends the Windows Logon Procedure by supporting TPM Machine Binding Features.

Features that can be installed with Runtime.msi		
Feature	**Feature Parent**	**Description**
RuntimeSys	---	Installs a runtime system.

Features that can be installed with Server.msi		
Feature	**Feature Parent**	**Description**
Server	---	Installs the SafeGuard Easy Server including Auditing.
SgeServer	Server	Installs the SGE Server.
RemAdmSupport	Server	Installs support for Remote Administration.
AdmConsole	Server	Installs the Administration Console.

4.4.2 SafeGuard Easy setup parameters

> ***NOTE:***
> You must use upper case letters to enter all the parameters in the command line syntax.

`AUTOBACKUP=0|1`

Specifies whether the Emergency Disk Wizard is to run automatically, to generate a system kernel backup, after a successful installation. By default it runs automatically (AUTOBACKUP=1).

`CFGFILE=`<configuration/migration file>

This parameter specifies the complete name of a SafeGuard Easy configuration file for an installation/migration.

`KERNELDRV=`<Name of the drive (C,D, etc.)>

Specifies the disk drive to which the SafeGuard Easy system kernel is to be saved. By default this is the Windows boot drive. It is a good idea to specify the disk drive to which the SafeGuard Easy system kernel is to be saved, for example, if you want to recover the Windows system partition with tools such as Ghost. Otherwise the restore would delete the SafeGuard Easy system kernel because the default setting is for it to be stored in the system partition

The target drive must be on the first hard disk!

`NOACTIVATION=0|1`

If NoActivation=1 although SafeGuard Easy files are copied to only one PC, the program itself is not activated. Not activated means that the master boot record is not exchanged and the SafeGuard Easy system kernel is not installed. SafeGuard Easy is activated afterwards from a configuration file with the "execcfg" command (e.g. execcfg /f:C:\SGE\Install.cfg). The default setting is for SafeGuard Easy to be active (NoActivation=0).

`PARTCHECK=0|1`

Specifies whether the partition types present support known file systems (FAT, FAT32, NTFS, etc.). If the partition type is unknown, the installation is cancelled. By default the check is active (PARTCHECK=1).

`SERVER`=<Server name>

Specifies the name of the workstation on which the SafeGuard Easy Server is installed. You can only use this parameter if the "Server connection" feature (which supports Central Administration on a client) has been selected for this installation.

`GROUPS`=<group name1,group name2, etc.>

Specifies the (SafeGuard Easy) groups to which the workstation is assigned in central administration, when they register on the SafeGuard Easy Server. You can only use this parameter if the "Server connection" feature (which supports Central Administration on a client) has been selected for this installation.

`GINASYS=0|1`

Specifies whether the SafeGuard GINA System is to be installed to control Windows logon. The default setting is that SafeGuard GINA is installed (GINASYS=1).

WARNING:

We recommend that you always implement the Utimaco GINA.
The Utimaco GINA system is an important element of SafeGuard Easy. The GINA system will gain even more importance in the future, as we plan to implement new functionality. If the GINA is not installed, some functionality will not be available for migration to the new version.
A missing GINA can even impair future migrations.

If you do not install the Utimaco GINA, some SafeGuard Easy functions will not be available after installation:

- The dialog for encryption/decryption (ECVIEW) will not be displayed if the user is not logged on.
- SAL logon and automatic smartcard logon do not work.
- Windows logon cannot be blocked with active Wake-On-LAN.
- Password synchronization between Windows and SafeGuard Easy does not work.

5 Update

If an earlier version of SafeGuard Easy is already installed on your workstation, you will find it easy to upgrade. If you do, any settings you have already made (user name, user password etc.) are reused.

You can update to the current version of SafeGuard Easy from all SafeGuard Easy versions >=4.11 (build no. 4.11.0.138).

You can either initiate migration during installation, or automatically, with the help of a preconfigured migration file. In both cases you use the Migration Wizard.

5.1 Local update

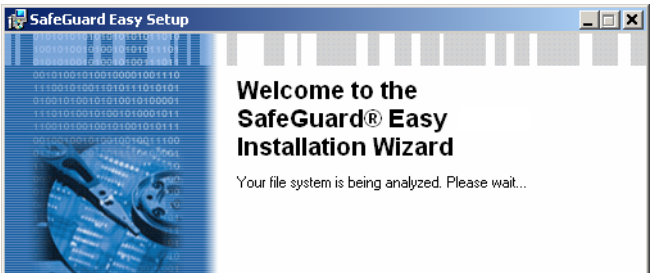
How to run a local update:

1. On the SafeGuard Easy program CD select the \Client folder and run `Setup.exe`.

2. SafeGuard Easy discovers that an older version is already installed on a workstation and displays a dialog to tell you.

SafeGuard Easy Setup
Welcome to the SafeGuard® Easy Installation Wizard
An installed older version of SafeGuard Easy was detected. The installation will perform an upgrade.

3. A program checks the system kernel.


SafeGuard Easy Setup
Welcome to the SafeGuard® Easy Installation Wizard
Your file system is being analyzed. Please wait...

4. If there are no problems in the system kernel, the update runs smoothly and the welcome screen appears.

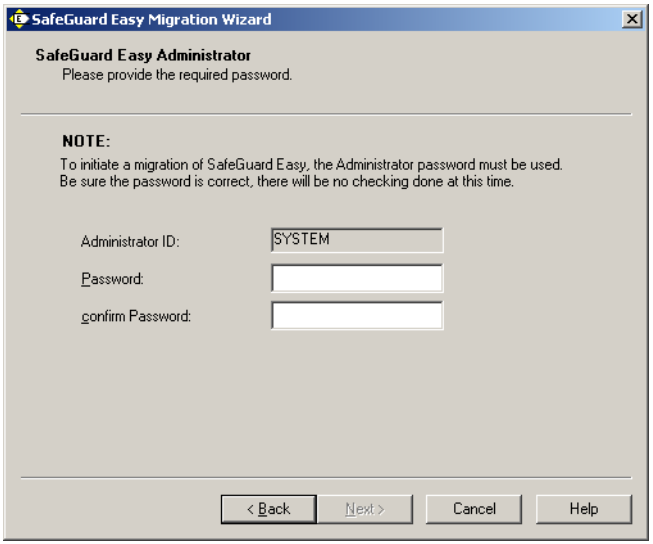
   If the system kernel is corrupt, it must be repaired.

5. Then, accept the terms of the licence agreement, specify the SafeGuard Easy installation directory and select the features (SAL, Server Connection etc.) you require.

6. The update starts.

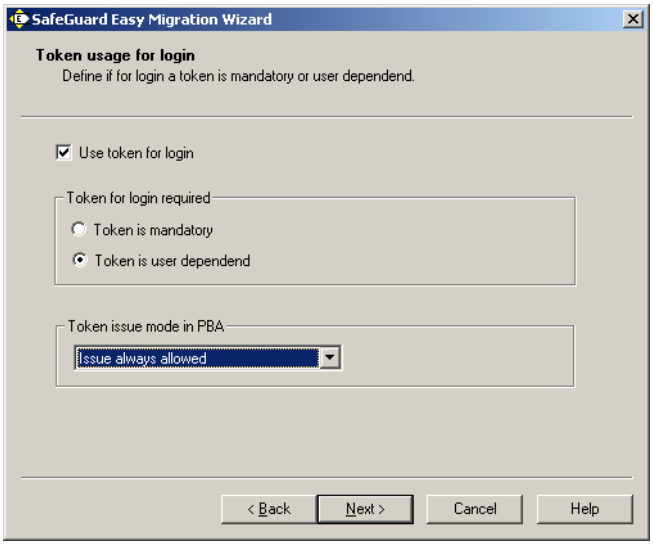
7. The "SafeGuard Easy Administrator" dialog appears.

   Only the "SYSTEM" SafeGuard Easy user can perform a migration on a workstation. Enter the appropriate SafeGuard Easy password for authentication.


SafeGuard Easy Migration Wizard
SafeGuard Easy Administrator
Please provide the required password.
NOTE:
To initiate a migration of SafeGuard Easy, the Administrator password must be used.
Be sure the password is correct, there will be no checking done at this time.
Administrator ID:
SYSTEM
Password:
confirm Password:
< Back
Next >
Cancel
Help

8. The "Token usage for login" dialog appears.

Versions of SafeGuard Easy before 4.0 did not support tokens. You can now "retrofit" this additional functionality during the update.


SafeGuard Easy Migration Wizard
Token usage for login
Define if for login a token is mandatory or user dependend.
Use token for login
Token for login required
Token is mandatory
Token is user dependend
Token issue mode in PBA
Issue always allowed
< Back
Next >
Cancel
Help

- **Use token for login**
  Specifies if token-based logon is supported or not.

  NOTE: If you want to enable token-based logon after an update, you will have to reinstall SafeGuard Easy.

- **Token for logon required**
  Specifies whether all SafeGuard Easy users must log on with a token, or only selected users.

  - *Mandatory:*
    Defines if token logon is required for all SafeGuard Easy users. If the token is lost, the Challenge/Response procedure cannot be used to provide remote help.

- *User-dependent:*
  This rule gives users increased flexibility, because the right to use a token can be granted or denied to them even after SafeGuard Easy has been installed.

- **Token issue mode in PBA**
  Specifies who is entitled to write SafeGuard Easy data to a token.

  - *Issue always allowed:*
    SafeGuard Easy user is allowed to issue the token.

  - *External permission required:*
    The Helpdesk is involved in the issuing process (using the Challenge/Response procedure).

  - *Issue is not allowed:*
    SafeGuard Easy user is not allowed to issue the token: it is issued centrally with Token Administration.

You will find more detailed information in the Token Support chapter.

9. The "Target directory" dialog appears.

   Specify the path on which you want to save the `SGEMig.cfg` migration file. The migration file contains the SYSTEM password and the settings for token support.

   The program recognizes the folder in which the previous version of SafeGuard Easy was stored and displays this path as the default. Click the [Browse] button to select which disk drive and folder the file is stored in.

   Click [Next] to create the migration file and start migration.

5.2 Unattended update with migration file

An automated update of SafeGuard Easy requires an migration file, which must be created with the Migration Wizard in the latest/new version of SafeGuard Easy. Then, to update SafeGuard Easy automatically, simply run the msiexec command line.

Creating a migration file

How to create a migration file

1. Install SafeGuard Easy's Configuration File Wizard on your Administrator PC. After this, the Migration Wizard is also installed.

2. Start the Migration Wizard with the `WIZLDR.exe` command in the SafeGuard Easy folder.

3. Enter all required data in the Migration Wizard's dialogs (see 'Local update').

4. The `SGEMig.cfg` file is created in the selected directory.

Command line (Example)

```
msiexec /i D:\Sgeasy.msi CFGFILE=D:\SGEmig.cfg /qn
```

Special case: Central Administration

If you want a SafeGuard Easy Client to be administered centrally with SafeGuard Easy tools after it has been updated, you must add the corresponding feature (ServerCon) and parameter (SERVER) in the command line, e.g.

```
msiexec /i D:\Sgeasy.msi ADDLOCAL=Sgeasy,Encryption,ServerCon
CFGFILE=D:\SGEmig.cfg SERVER=Server01 /qn
```

NOTE:
If you want to add Central Administration (Server Connection) to a SafeGuard Easy client after an update, you must re-install SafeGuard Easy.

After the update

After the update the client restarts and migration is complete.

5.3 System kernel check when there is an update

For an update to be successful, the SafeGuard Easy system kernel must be intact. From Version 4.20.1 SafeGuard Easy will check this before each update, and display a message for the user in the Setup dialog ("Your file system is being analyzed, please wait...").

If the system kernel is OK, the update will run without any problems.

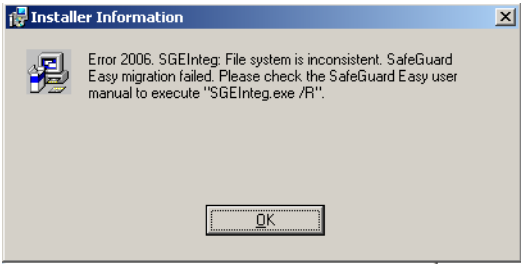
If the system kernel is not OK, the system displays an error message that indicates possible problems and recommends that you run a repair program (SGEInteg) before the update.

5.3.1 What happens if the system kernel is not OK?

1. Run SafeGuard Easy Update.

2. The SGEInteg repair program runs in the background, analyzes the system kernel and discovers that it is not OK.

3. It displays a dialog message ("SGEInteg: File system is inconsistent. The SafeGuard Easy migration failed. Please check the SafeGuard Easy user manual to execute SGEInteg /R.").


Installer Information
Error 2006. SGEInteg: File system is inconsistent. SafeGuard Easy migration failed. Please check the SafeGuard Easy user manual to execute "SGEInteg.exe /R".
OK

   The setup stops at this point. During an automatic installation the error number “2006” is written to the Windows Installer log file (logging must be switched on).

4. Run "SGEInteg /R" on the command line. You will find the SGEInteg program in the \Tools folder on the SafeGuard Easy CD.

5. SGEInteg repairs files and the file system in two steps: First it repairs all file errors that do not require a restart. Then, if it finds file errors that require a restart, SGEInteg triggers the checking of the hard disk (chkdsk). If the user agree that the computer should be restarted, chkdsk runs.

5.3.2 About the repair program

The repair program runs automatically when you trigger an update to the current version of SafeGuard Easy. A user/administrator can also run it manually (for example, with an additional parameter) from the Tools folder on the CD.

When it is run with the parameter /R, SGEInteg repairs the file system. SGEInteg reports both repairable and fatal errors. If a repair is performed, it may also then be necessary to run the chkdsk program to check the hard disk. Usually, the computer then reboots.

5.3.3 Parameters for the repair program

SGEInteg can be called with these parameters:

```
SGEINTEG [/?] [/c] [/r] [/p] [/d] [/len] [/v] [/y]
```

/?	Help Displays all parameters.
/c	Starts the analysis of the file system.
/r	Activates Repair mode Any file system errors it identifies will be repaired. If you call "SGEInteg /R", the system also runs the '/P' parameter and performs a file system analysis. However this may result in a reboot.
/p	Corrects the SafeGuard Easy path details in HKEY_LOCAL_MACHINE SOFTWARE Microsoft Windows CurrentVersion Run Older versions of SafeGuard Easy enter path details in this registry entry without quotation marks. This may mean that these programs cannot be run in newer versions of Windows. SGEInteg uses this parameter to correct the path details. You must then reboot the computer. If you call 'SGEInteg' without parameter, the system corrects the path details and performs a file system analysis.

/d	Restores the CRAREA Registry entry. Older versions of SafeGuard Easy had difficulties generating this Registry entry during installation. If the Registry entry is not present this can cause problems during uninstall and updates to new versions. SGEInteg /d restores the entry in HKEY_LOCAL_MACHINE SOFTWARE Utimaco SGEasy CRAREA
/len	Fixes a problem involving Rescue and Recovery (RnR) When an update is performed to the current version of SafeGuard Easy, the following problem can occur if RnR is installed: The 'SGEDemon.exe' program is displayed after each restart and then stops running. As SGEDemon.exe is only needed once after the update, it can be switched off without any negative consequences. SGEInteg /len removes SGEDemon.exe from HKEY_LOCAL_MACHINE SOFTWARE Microsoft Windows CurrentVersion Run
/v	Activates Verbose mode Verbose mode displays more detailed status/error messages on screen.

/y	Activates unattended mode All dialogs are automatically confirmed with YES.

/V	Activates verbose mode Verbose mode displays more detailed status and error messages on screen.
/R	Activates repair mode. In this mode, the system repairs identified file system errors. If 'SGEInteg /R' is run, the path details (parameter /P) and a file system analysis are run, unattended, in the background. The system may be rebooted.
/Y	Activates unmonitored mode In this mode, all dialogs are automatically confirmed with yes.
/P	Corrects the SafeGuard Easy path details in HKEY_LOCAL_MACHINE SOFTWARE Microsoft Windows CurrentVersion Run Older versions of SafeGuard Easy insert path details in this registry key without quotation marks. In newer versions of Windows, in some circumstances, this can prevent these programs from being executed. When this parameter is used, SGEInteg corrects the path details. You should then reboot the computer afterwards. If 'SGEInteg' is run without any parameter, the system corrects the path details and runs a file system analysis.

6 Uninstallation

The uninstallation of SafeGuard Easy has the following effects:

- All formerly encrypted areas of the hard disk(s) are decrypted.
- Pre-Boot Authentication is removed, if installed.
- The original Windows logon appears again if SAL was installed.
- All SafeGuard Easy files are deleted.
- All SafeGuard Easy registry entries are removed.

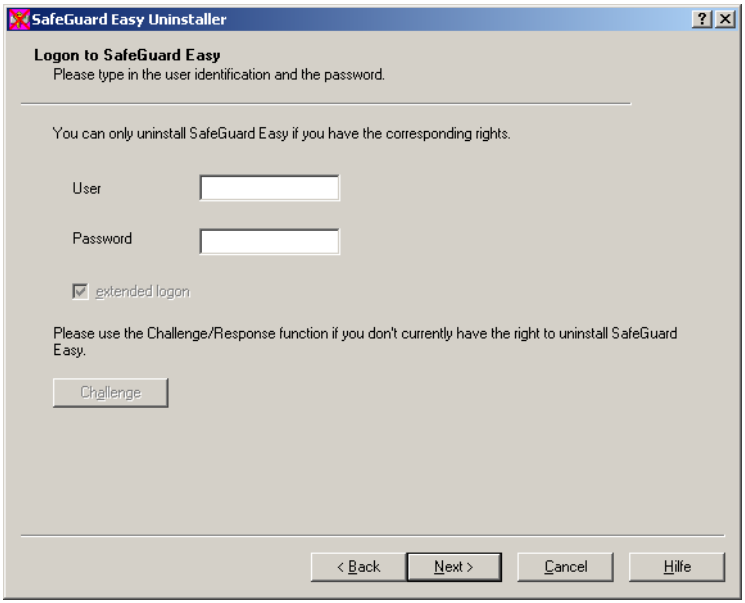
By default, SafeGuard Easy can only be uninstalled by the SYSTEM user. If another person has been granted the uninstall right, this person can also carry out an uninstall.

Do not attempt to remove SafeGuard Easy by simply deleting the files. If SafeGuard Easy is not uninstalled correctly, its registry entries will remain. This may prevent SafeGuard Easy from being re-installed. In this case you must re-install your operating system.

6.1 Local uninstallation

Select Start/Settings/Control Panel/Add/Remove Programs and then "SafeGuard Easy" (or also SafeGuard Easy features such as Server or Runtime).

If you select [Remove] and click [Next], in the welcome screen, you access the Logon to SafeGuard Easy dialog.


SafeGuard Easy Uninstaller
Logon to SafeGuard Easy
Please type in the user identification and the password.
You can only uninstall SafeGuard Easy if you have the corresponding rights.
User
Password
extended logon
Please use the Challenge/Response function if you don't currently have the right to uninstall SafeGuard Easy.
Challenge
< Back
Next >
Cancel
Hilfe

The user who wants to uninstall the program is prompted to enter their SafeGuard Easy user name and password. This user must have the right to remove SafeGuard Easy. After entering the correct user data, click [Next] and confirm the security check. SafeGuard Easy will be removed automatically.

6.2 Uninstall with Challenge/ Response

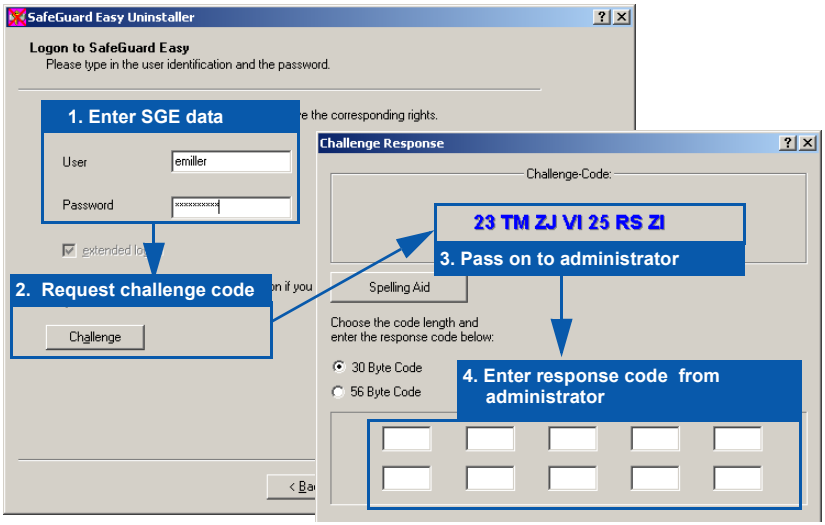
If a SafeGuard Easy user is not authorized to uninstall SafeGuard Easy, according to their user profile, the Administrator can assign them this right by using the Challenge/Response procedure. To do this, the user and the administrator exchange a challenge code and response code.

The person generating the response code (Administrator) must know a SafeGuard Easy user profile on the user PC that is permitted to uninstall SafeGuard Easy. This user profile must also always have *at least the same rights* as the user, on the user's computer.

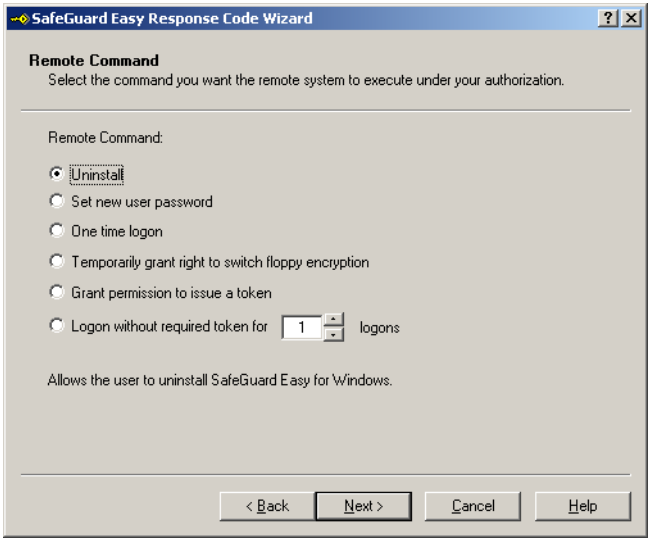
How to uninstall SafeGuard Easy with Challenge/Response:

1. The user initiates the uninstall procedure (see 'Local uninstallation') and reaches the *Logon to SafeGuard Easy* dialog.

2. In *Logon to SafeGuard Easy* dialog, they enter their SafeGuard Easy data, request the challenge code and use the telephone, SMS or e-mail to pass it to the administrator.



3. The administrator uses the Response Code Wizard to generate a response code containing the SafeGuard Easy access data of the user (in the example above, user "emiller"). The response code is assigned the right to uninstall SafeGuard Easy.


SafeGuard Easy Response Code Wizard
Remote Command
Select the command you want the remote system to execute under your authorization.
Remote Command:
Uninstall
Set new user password
One time logon
Temporarily grant right to switch floppy encryption
Grant permission to issue a token
Logon without required token for
1
logons
Allows the user to uninstall SafeGuard Easy for Windows.
< Back
Next >
Cancel
Help

4. SafeGuard Easy is uninstalled once the challenge code and response code have been exchanged.

6.3 Unattended uninstall with configuration file

Uninstalling SafeGuard Easy can be automated if the `MSIEXEC` command is used to run a configuration file with the property "uninstall".

Command line syntax

```
msiexec /x D:\SGEasy\Sgeasy.msi CFGFILE=D:\Uninstall.cfg /qn
```

7 System boot and logon

Before Windows' own authentication mechanism loads, SafeGuard Easy displays a logon dialog. This is the **Pre-Boot Authentication (PBA)**. Logon to PBA is the default method after installation.

If Pre-Boot Authentication is enabled, a user can only log on with their SafeGuard Easy access data. The password a user enters is used to calculate the key that is required for booting: the key is used to decipher an encrypted hard disk.

If Pre-Boot Authentication is disabled, the hard disk will still be encrypted, but boot without any user interaction at the Windows logon screen. This option requires that hidden Pre-Boot (SafeGuard Easy) credentials are stored on the hard disk itself and therefore has a lower security level than a system that runs PBA.

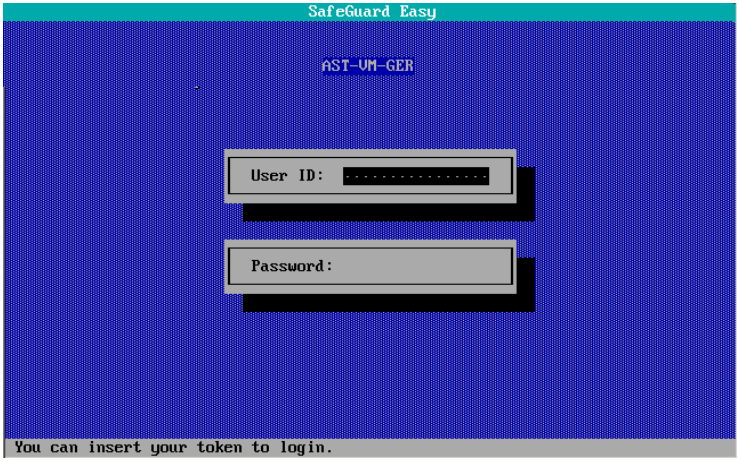
Users can log on to PBA

- as a regular user (with user name and password)
- as a default user (with password only)
- with a token (with a token password)

The PBA logon screen has these features and functions:

- Name of the workstation and text for legal information
- Help function for changing the SafeGuard Easy/token password
- Help function for resetting forgotten passwords

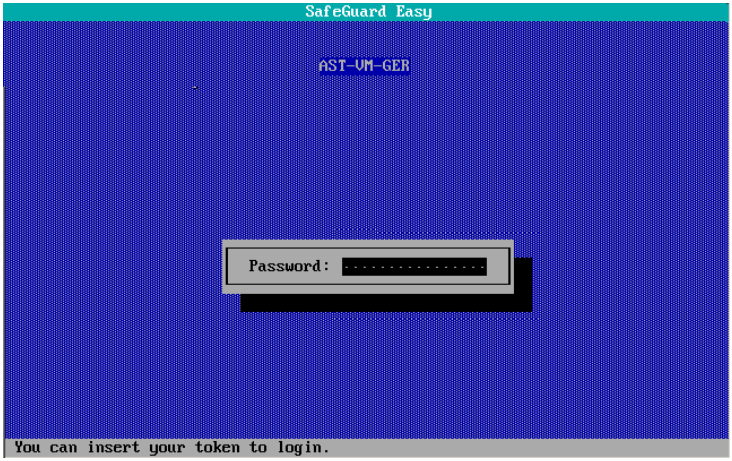
7.1 Logging on as a regular user



Normally the user logs on to PBA with their SafeGuard Easy user name and password.

Under the product name, the name of the workstation is displayed (in this example, "AST-VM-GER"). This data is taken from the system settings for your workstation.

7.2 Logging on as a default user



If any SafeGuard Easy user is set as a "default user" on a workstation, they are only prompted for the SafeGuard Easy password. They do not need to enter their user name.

7.2.1 Extended logon via function key [F2]

If someone other than the default user wants to log on, then *extended logon* must be switched on. This means that, in addition to the SafeGuard Easy password, they will also have to enter their user name.

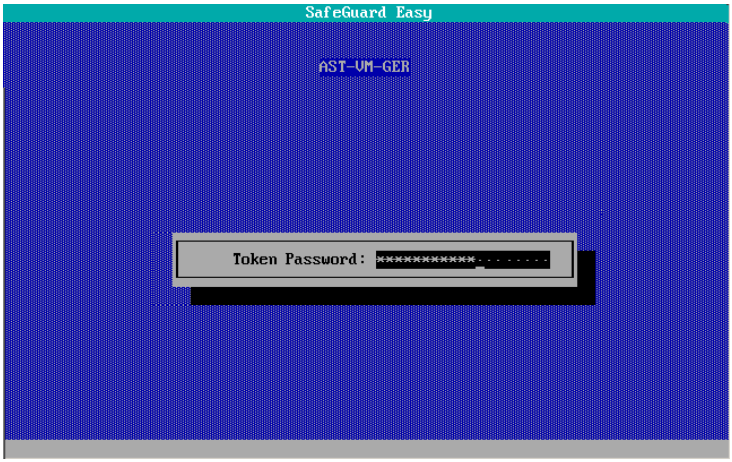
If they press [F2], the field in which they enter their user name is displayed above the field in which they enter their password.

> ***WARNING:***
> The SYSTEM user must **always** log on with their user name and password.

7.3 Logging on using a token

SafeGuard Easy allows you to log on to PBA using a token. This is a quick and easy way of logging on to your PC.

If a USB token has been inserted in your PC, the PBA dialog displays an input field in which you enter the password for your token. When you confirm your entry, the system compares the input to check whether the SafeGuard Easy user saved on the token is present on the PC. If the data matches, the system logs you on.



7.4 Changing the SafeGuard Easy password via the [F10] key

Users can change their own SafeGuard Easy password independently by pressing [F10]. To do so, the user enters their current SafeGuard Easy data and confirms it by pressing [F10]. Then they see a prompt at which they enter their new password.

Alternatively, the SafeGuard Easy administrator can specify that users have to define a new password after a certain amount of time has passed.

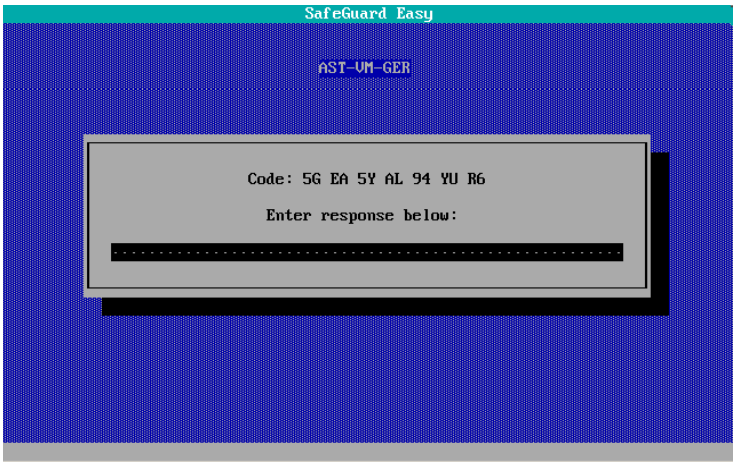
If a user logs on using a token, they can press [F10] to change the token password, but the SafeGuard Easy data on the token will not be changed.

7.5 Help function for resetting forgotten passwords via the [F9] key

SafeGuard Easy includes a Challenge/Response procedure for resetting "forgotten" passwords. If a user requires help, they must generate a challenge code in PBA by pressing [F9].

This challenge code is displayed as an ASCII character string (14 characters) on the user's screen. The user then calls their administrator and tells them their user information and the challenge code. The administrator then generates a response code. When the user enters this response code on their PC they can reset their password.

For details of the Challenge/Response procedure, please read Chapter 'Remote maintenance (Challenge/Response)'.



7.6 Failed logon

Login fails if

- The SafeGuard Easy user name is incorrect
- The SafeGuard Easy user password is incorrect or
- The user name has expired

If a user enters their PBA password incorrectly, the waiting period increases after the second logon attempt. The waiting period can be reset by a valid logon.

Resetting a failed logon

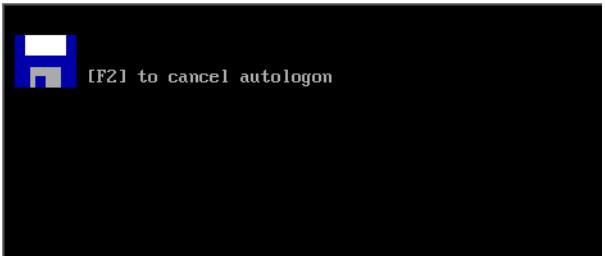
You can reset the waiting period as follows:

1. Insert the emergency disk and boot the system from the A: drive.
2. Run the `Sgeasy.exe` program.
3. Type in the SafeGuard Easy user password.
4. In the next menu you see (Options Uninstall, Repair, Restore), select "Cancel".
5. Reboot the system.

This resets the waiting period.

7.7 Pressing [F2] to force logon with PBA

If PBA is switched off, you can wait until a floppy disk icon appears in the top left-hand corner of the monitor, and then press [F2] to call PBA and log on in the usual way.

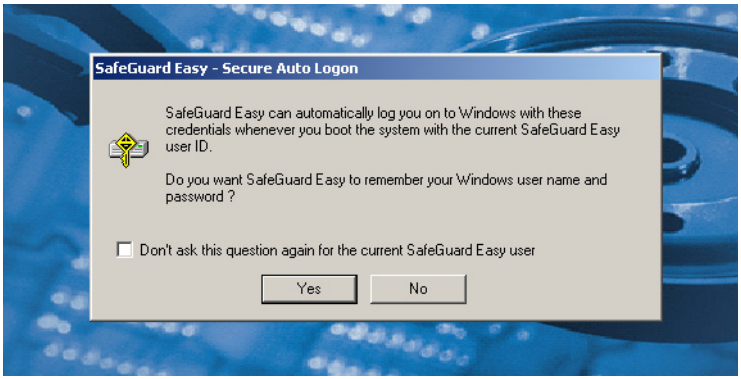


7.8 Logging on to the operating system automatically

If required, SafeGuard Easy can carry out an automatic logon to Windows. SafeGuard Easy calls this function *Secure Automatic Logon* (or SAL for short). Once the Windows data has been entered, the SAL places it in a protected area and loads it again whenever the user successfully logs on in PBA.

The only prerequisite for SAL is that PBA is switched on.

The SAL dialog is displayed after logon to the operating system.


SafeGuard Easy - Secure Auto Logon
SafeGuard Easy can automatically log you on to Windows with these credentials whenever you boot the system with the current SafeGuard Easy user ID.
Do you want SafeGuard Easy to remember your Windows user name and password ?
Don't ask this question again for the current SafeGuard Easy user
Yes
No

If the user selects automatic logon, they will only need their SafeGuard Easy data to log on in the future.

SAL can also be used with smartcards.

For details of Automatic Logon, please read Chapter 'Configuring Windows logon'.

7.9 Compatibility with logon components supplied by other vendors

To guarantee the best possible security, the Utimaco Logon component ensures that it is always the first Windows logon component called by the operating system. Should anything change the call order the Utimaco Logon component will automatically reinstate itself as the first component to be called. If, as a result, logging on to Windows becomes impossible, or Windows no longer responds after logging on, there are two possible ways to undo the changes introduced by the logon component:

- To manually define the logon component that is to be called by Utimaco logon component, press and hold down [F8] key when the system first switches from the blue text display to the (as yet empty) desktop.
- If [F8] is not pressed, a dialog will appear. The user must define the logon component that is to be called by the Utimaco logon component, either the original Microsoft logon component or a third-party logon component. This dialog will reappear at each login until the user disables it. After that, the current logon component setting remains. Selecting the original Microsoft component will ensure that logon is performed correctly but may disable some features of the third-party product. Due to a lack of standardization it is not always possible to run every set of different Windows logon components together.

For bigger rollouts it is possible to suppress this user interaction. To do so the administrator must ensure that, before the reboot after the new logon component has been installed, the "ForceKnownGina" registry value in the "HKLM\Software\Utimaco\SGLogon" key is set from 0 to the value 1 (new logon component will be called by SafeGuard Logon Extensions). Alternatively, you can set this value to 2 to force the use of the original Microsoft component even if other software is installed.

8 Administration overview

You can configure SafeGuard Easy using the Configuration File Wizard or the SafeGuard Easy Administration function. By using the Administration function you gain direct access to the PC's SafeGuard Easy configuration. This is ideal for local administration on a single PC. The Configuration File Wizard does not change the local settings but collects SafeGuard Easy settings in a file which is then distributed to clients.

These administration programs have very similar settings. In both programs, the user must authenticate themselves with the correct SafeGuard Easy data before they can make any changes.

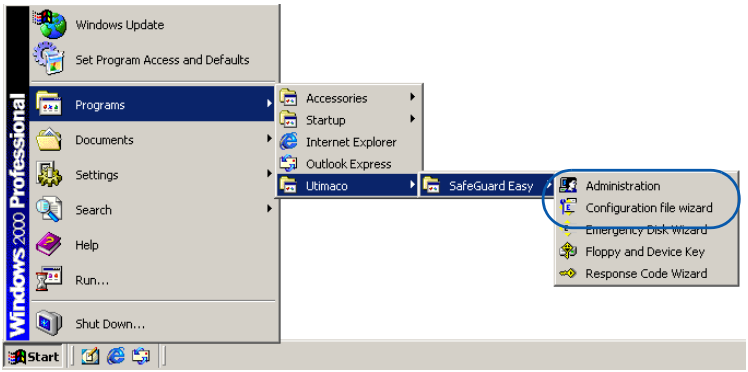
Which of the two programs you use depends on your individual situation, and is described below.

8.1 Separation of functions

First you must specify whether the functions of the system administrator are to be combined with the functions of the "simple" user, or kept separate. If the functions are kept separate, you can integrate one or more administration aids.

- **Combined function:** The user is also the system administrator. The user configures SafeGuard Easy on their PC for their own use (one person). All settings are made in the Administration function. The configuration program is not required. There is no need to create a configuration file.
- **Separate functions on one PC:** The system administrator configures SafeGuard Easy on the user PC. If the system administrator creates an "administrator" account, in addition to the "user" account, three people then have access to the PC. The Administration function is used to set up configuration. The configuration program is not required as no configuration file has to be created.
- **Separate functions on several PCs:** The system administrator configures SafeGuard Easy on their own PC for several workstations. An administration utility can be used for the other admin tasks. For this task you use the Configuration File Wizard to create a file in which the definitions are saved. A preconfigured installation is used to pass on the configuration file to the user PCs. If you want to use other settings on the system administrator PC, you also use the Administration function.

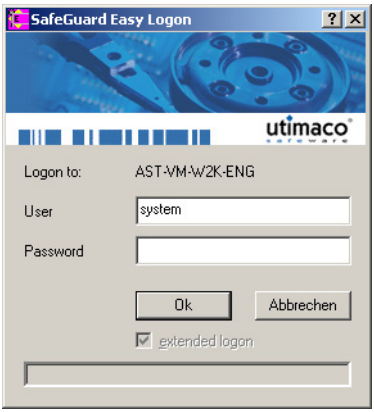
8.2 Starting the Administration function and the Configuration File Wizard



After a complete installation, SafeGuard Easy creates a folder called SafeGuard Easy in Programs/Utimaco. You can use it to run the Administration function and the Configuration File Wizard.

8.3 The Administration function

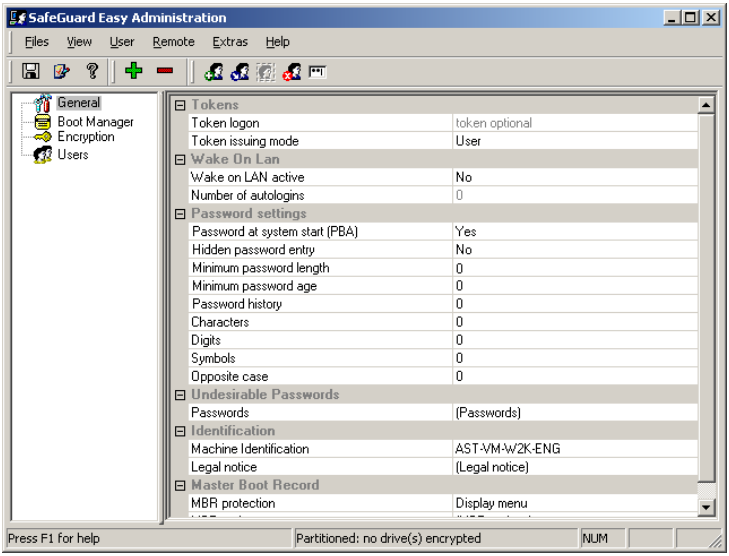
After the Administration function runs, you see the logon dialog. Here you must enter valid SafeGuard Easy data before you can access the Administration function.



You cannot make more than five logon attempts. After five unsuccessful attempts, you must restart the system and try logging on again.

8.3.1 Administration window

When you have correctly entered the SafeGuard Easy user data, the Administration window opens.



The left-hand pane shows a list of all available configuration pages. If you select a configuration page in the left-hand pane, its details are displayed in the right-hand pane. The settings are the same as those you can make while installing SafeGuard Easy.

The bottom section of the Administration window displays additional information:

- Encryption mode and the encryption status of the disk drives (in the figure: Partitioned, no drive(s) encrypted).
- The status of the keys for the number pad and the Shift key (in the figure, you see "NUM", as number lock is selected).

By default, any user logged on to the Administration function can change their SafeGuard Easy password. Other rights depend on the user's rights profile.

8.3.2 Toolbar

The Administration function has a toolbar with buttons for the most important commands:

- **Save**
  Stores new settings. If changed settings mean that the must be PC rebooted, a dialog is displayed.
- **Configure Workspace**
  Ensures that, when the Administration function is opened after the next logon, it is in exactly the same state as when it was closed (same window size and position, same configuration page, etc.).
- **Help**
  Displays the online help.
- **Plus/Minus characters**
  In the right-hand pane the plus character displays all subordinate settings, and the minus character minimizes the view to the settings titles.
- **Create user**
  Creates a new user (display depends on the rights profiles of the user who is currently logged on).
- **Copy user**
  Copies an existing user (display depends on the rights profiles of the user who is currently logged on).
- **Delete user**
  Removes the user from the list (display depends on the rights profiles of the user who is currently logged on).

- **Change password**
  The logged on user can use this to change their password.

You can also access all these commands via the menus (Files, View, User, Extras, Help).

8.4 Configuration File Wizard

The Configuration File Wizard has only one task, to generate files that automate the installation and removing of SafeGuard Easy. Even administrative tasks such as changing an existing SafeGuard Easy installation can be triggered using configuration files. In network environments, the administrator sends the configuration files to the user PCs and runs them there without user interaction. After the same configuration file has been run on several PCs, SafeGuard Easy uses the same configuration on all of them.

A configuration file is system-independent, so it can also be used on other systems besides the one on which it was generated. However, the same SafeGuard Easy version must be present on all the workstations that are being configured.

NOTES:

You only need the administration tools to generate a configuration file. When you generate a configuration file, SafeGuard Easy is not installed on your computer.

SafeGuard Easy only supports configuration files generated with the current Configuration File Wizard.

Configuration files must be protected from unauthorized access. Regular users must not access configuration files.

8.4.1 Reuse of configuration files from older versions of SafeGuard Easy

Configuration files from earlier versions can be read and imported to the Configuration File Wizard without any difficulties, provided that the files

- were created with a Configuration File Wizard from SafeGuard Easy version 3.20 onwards.
- have the file type "Install".

If you load an older file, SafeGuard Easy will also automatically display the new configuration options (for example, new features since version 3.20 include token-based logon) and sets them as default values.

8.4.2 Creating a new configuration file

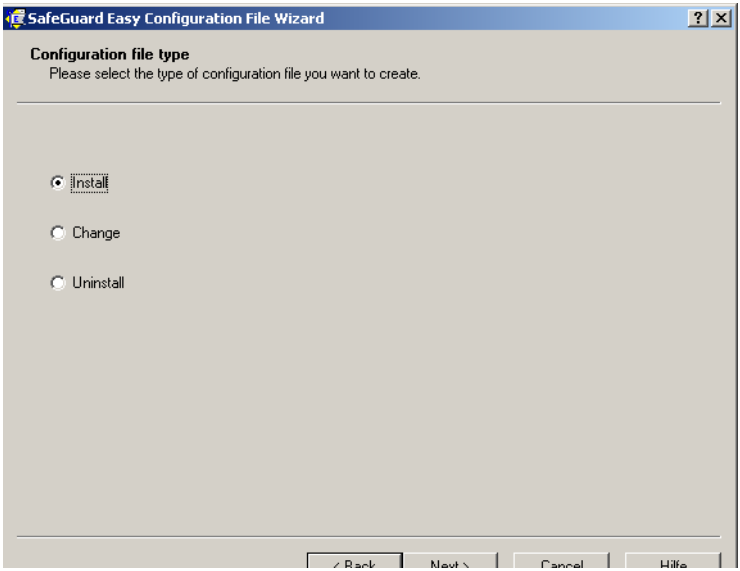
You use the Configuration File Wizard to generate files for installing and removing SafeGuard Easy without user interaction. Step-by-step, the Configuration File Wizard records the information that a file should contain.

To generate new configuration files, select Start/Programs/Utimaco/SafeGuard Easy/**Configuration File Wizard**.

In the Wizard, click [Next] to confirm that all the entries are correct.

After you run the Wizard you must then decide what purpose the configuration file is to be generated for.

- Installation
- To change an existing SafeGuard Easy installation ("delta" file)
- Uninstall

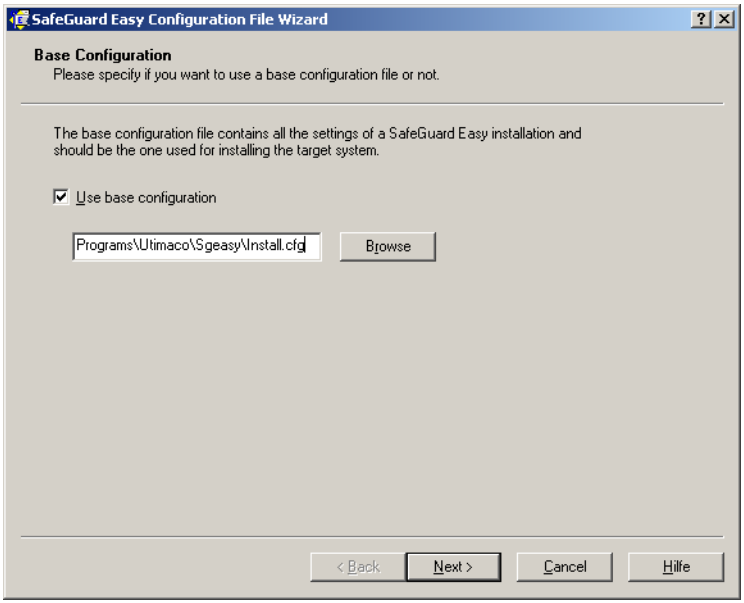


8.4.3 Creating a configuration file for installation

Select the "Install" attribute to generate a configuration file that installs SafeGuard Easy automatically on a client (see 'Central installation').

After you select "Install" the first thing you specify is whether a base configuration is to be used for the new configuration file.

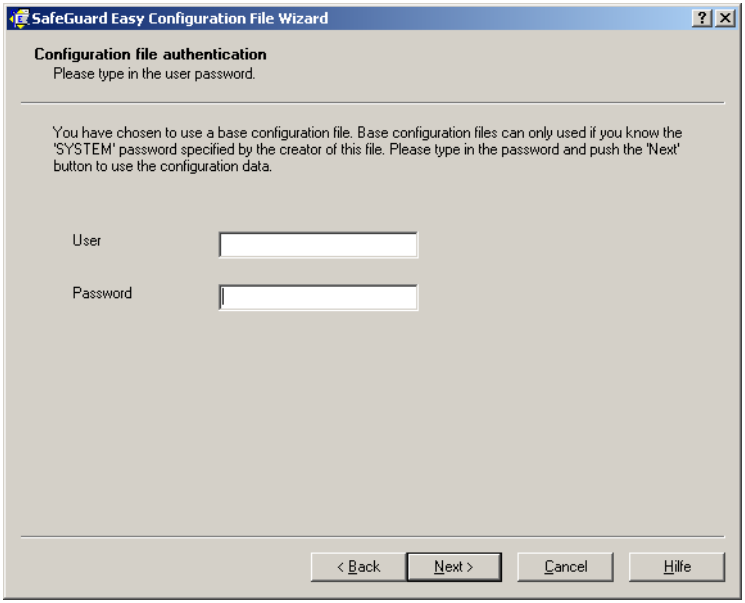
Base configuration


SafeGuard Easy Configuration File Wizard
Base Configuration
Please specify if you want to use a base configuration file or not.
The base configuration file contains all the settings of a SafeGuard Easy installation and should be the one used for installing the target system.
Use base configuration
Programs\Utimaco\Sgeasy\Install.cfg
Browse
< Back
Next >
Cancel
Hilfe

A base configuration file is an existing configuration file with the attribute "Install". It is used as a template/basis for a new installation file.

Authentication to the base configuration file

The settings for a selected base configuration file are not visible until the SafeGuard Easy user SYSTEM has logged on.

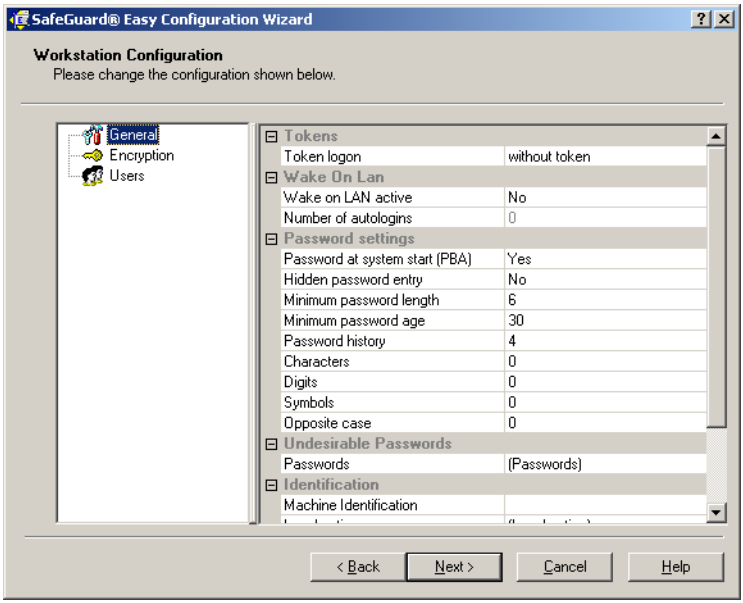

SafeGuard Easy Configuration File Wizard
Configuration file authentication
Please type in the user password.
You have chosen to use a base configuration file. Base configuration files can only used if you know the 'SYSTEM' password specified by the creator of this file. Please type in the password and push the 'Next' button to use the configuration data.
User
Password
< Back
Next >
Cancel
Hilfe

Encryption mode

If a base configuration file is not used, the new configuration file must be assigned an encryption mode so that SafeGuard Easy knows which hard disk areas are to be encrypted (see 'Encryption mode').

Configuration

You then see a window that displays the different configuration pages. If a base configuration file is used, its settings are loaded. If not, the default settings are displayed.



You will find a detailed description of the configuration pages in the relevant chapters.

Target directory

In the Target directory dialog you can specify where you want to store the configuration file.

To avoid problems we recommend that you write down the details of the configuration file settings.

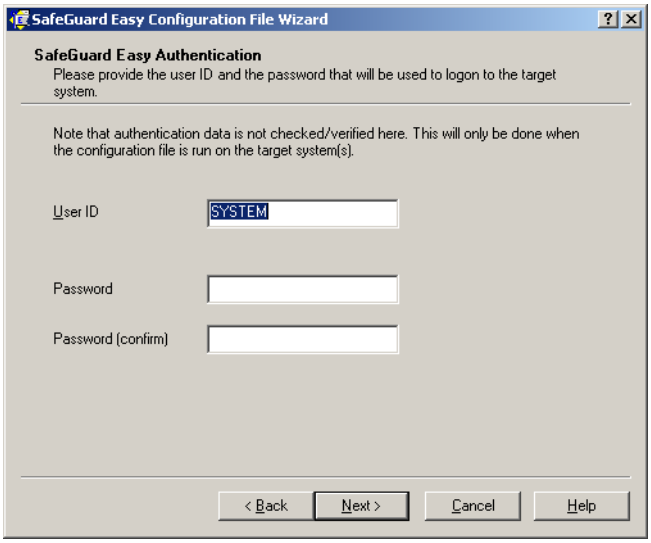
Note about the "Change" file type with the base configuration file:

If you click [Save], you are prompted to confirm that you want to replace the existing base configuration file. If you do so, by clicking [Yes], all changes will be written to the existing base configuration file.

Here we recommend that you create a new base configuration file, so that you can retain your original base configuration file.

8.4.4 Creating a configuration file for removing SafeGuard Easy

The configuration type "Uninstall" opens the SafeGuard Easy Authentication dialog.


SafeGuard Easy Configuration File Wizard
SafeGuard Easy Authentication
Please provide the user ID and the password that will be used to logon to the target system.
Note that authentication data is not checked/verified here. This will only be done when the configuration file is run on the target system(s).
User ID
SYSTEM
Password
Password (confirm)
< Back
Next >
Cancel
Help

The user entered here must be present on the workstation, on which the configuration file is being run, and have the "Uninstall" right.

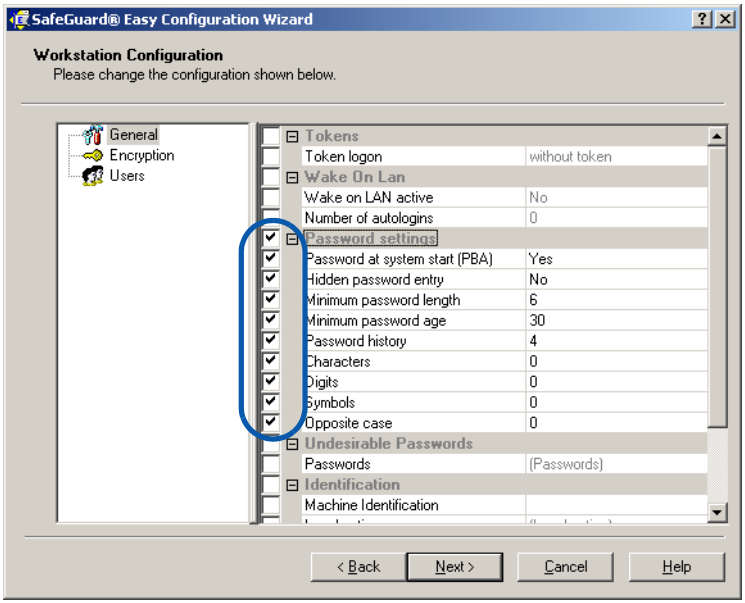
When you have entered all the data, click [Next]. The Wizard opens the *Target directory* dialog. Here you give the configuration file a name.

8.4.5 Creating a configuration file for a change installation ("delta file")

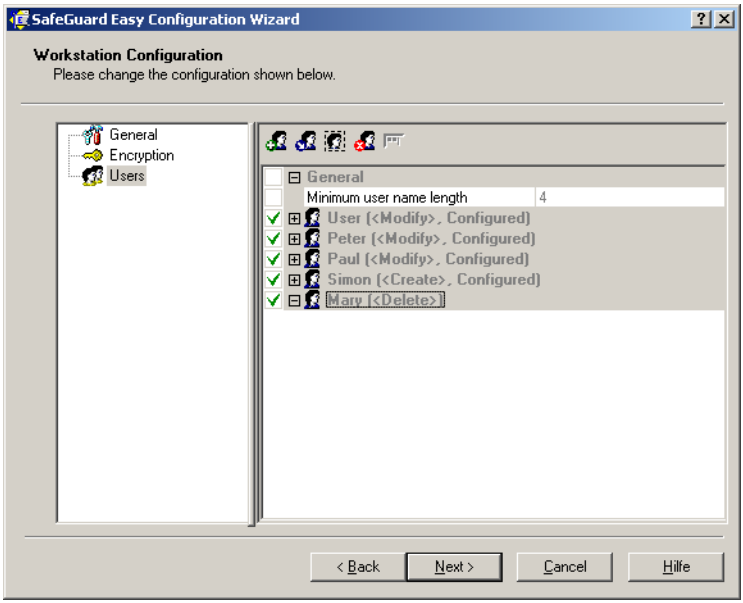
Essentially, a delta file changes the settings of an existing SafeGuard Easy installation. You can also use a base configuration in the same way as an installation file, to create a delta file, if required.

However, unlike an installation file, you cannot change the status of hard disk encryption and token support in a delta file.

To change the options on the individual configuration pages for a delta file, first click the appropriate check box.



On the *Users* configuration page, please note the functionality of the buttons for creating, copying and deleting users.



- **Create user**
  When you run the configuration file, this option generates a new SafeGuard Easy user on the target machine (in this example, the user *Simon*).

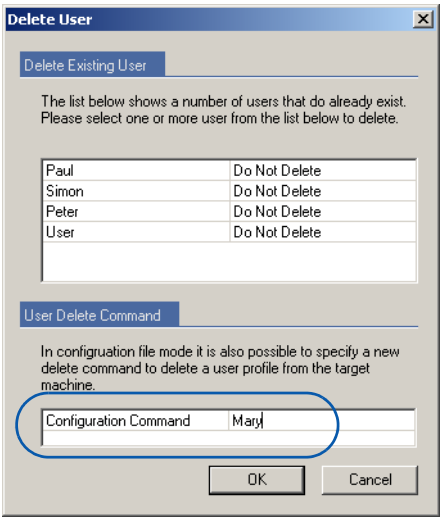
- **Copy user**
  Takes all settings from the copied entry, and the new SafeGuard Easy user is also assigned the attribute "Create".

- **Change user**
  Generates a user who is already present on a target machine and assigns new properties to that user (in this example, users *User, Peter* and *Paul* with the attribute "Modify").

  All users loaded from a base configuration automatically have the "Modify" attribute. If a base configuration is not used, users must first be generated with this attribute.

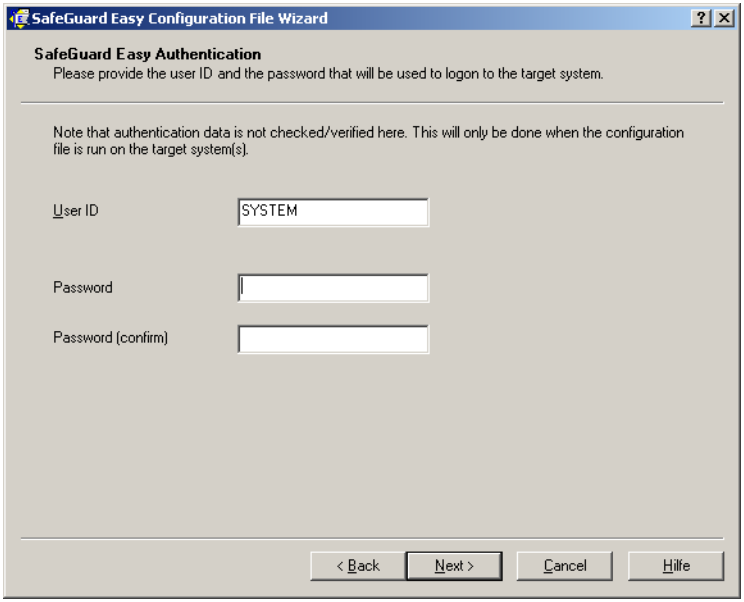
- **Delete user**
  Specifies the name of an existing user, who is then deleted when the configuration file is run on this target system (in this example, User *Mary*).

NOTE:
In delta files without a base configuration, use the "Configuration command" field to "Delete" a user from the target system.


Delete User
Delete Existing User
The list below shows a number of users that do already exist. Please select one or more user from the list below to delete.
Paul
Do Not Delete
Simon
Do Not Delete
Peter
Do Not Delete
User
Do Not Delete
User Delete Command
In configuration file mode it is also possible to specify a new delete command to delete a user profile from the target machine.
Configuration Command
Mary
OK
Cancel

When you have entered all the data, click [Next]. The Wizard opens the *Authentication dialog* and then the *Target directory* dialog. Here you give the configuration file a name.

Authentication


SafeGuard Easy Configuration File Wizard
SafeGuard Easy Authentication
Please provide the user ID and the password that will be used to logon to the target system.
Note that authentication data is not checked/verified here. This will only be done when the configuration file is run on the target system(s).
User ID
SYSTEM
Password
Password (confirm)
< Back
Next >
Cancel
Hilfe

The SafeGuard Easy user you enter in the “Authentication” dialog must be present on the target machine and have the appropriate rights.

8.4.6 Run the delta file

How to run the delta file:

1. Start MS DOS mode.

2. Switch to the SafeGuard Easy directory.

3. Enter the command

   `EXECCFG.EXE /f:`*<Path and name of configuration file>*

   in the command line and then click [OK].

   Parameters regarding `EXECCFG.EXE` are displayed with the command `EXECCFG.EXE /?`

Additionally EXECCFG supports the /Reboot parameter that issues a shutdown after the defined configuration file has run successfully.

Example:

```
C:\SGEasy\EXECCFG /f:D:\Delta.cfg /Reboot
```

This command calls the delta file and issues a reboot.

Do not leave blank spaces between "`/f`" and the delta file's folder name!

8.4.7 Changing a configuration file

You can also change the settings of configuration files with the "Install" attribute at a later point in time.

How to change a configuration file:

1. Run the Configuration File Wizard.

2. Select file type "Install" and load the file you want to change in the *Base configuration* dialog.

3. Click [Next] to load the configuration file.

4. The settings stored in it are displayed and you can change them.

If you attempt to load a file that has the attributes "Modify" or "Delete", an error message is displayed.

8.5 Command line syntax for creation of a configuration file

If you want to perform unattended creation of a configuration file, use the `CfgWiz` program. `CfgWiz` comes as standard with SafeGuard Easy.

`CfgWiz` can be called with these parameters:

`/cmd:install | change | uninstall`

This option replaces the CFGWIZ Configuration file type dialog.

`/base:<filename>`

This option names the input configuration to be used. For install, this option replaces the CFGWIZ Base Configuration dialog. For change, this option replaces the install configuration selection dialog.

`/instfile:<filename>`

The name of the install configuration to be generated as output. When present, the administrator is not prompted for the save. If the file already exists, it is overwritten with the new configuration.

`/changefile:<filename>`

The name of the change configuration to be generated as output. When present, the administrator is not prompted for the save. If the file already exists, it is overwritten with the new configuration.

`/uninstfile:<filename>`

The name of the uninstall configuration to be generated as output. When present, the administrator is not prompted for the save. If the file already exists, it is overwritten with the new configuration.

Example:

```
CfgWiz /cmd:change /base:C:\install.cfg /instfile:C:\Change.cfg
```

NOTE:

These functions may be provided in future versions of LANDesk Management Systems.

8.5.1 Examples of use

Example 1:

You use the Configuration File Wizard to generate a file with which SafeGuard Easy can be installed on several workstations in a company without user interaction. The configuration file should also support a hierarchical administration concept and contain the following user profiles:

- SYSTEM: SafeGuard Easy administrator who has all the rights.
- SUBADMIN: sub-administrator to whom administrative tasks are delegated. Can change user settings and toggle floppy disk encryption.
- USER: end user who has no rights.

Procedure:

1. Run the Configuration File Wizard.
2. Select configuration file type "Install".
3. Select no base configuration.
4. Select "Full disk encryption" encryption mode.
5. Select General/ Password settings/Password at system start.

6. In User Settings, make the following settings:

   - SYSTEM (Password: System)
     Rights: All

   - SUBADMIN (Subadmin)
     Issue abbreviated C/R Code: YES
     Rights
     - Change user settings
     - Toggle floppy disk encryption

   - USER (User)
     Rights: none

7. In Encryption Settings, make the following settings:

   Floppy disks: ON
   Hard Disks: ON
   Removable Media: ON

8. In MBR Settings, leave the default settings unchanged.

9. Save as target folder base configuration file "Install.cfg".

10. Distribute Install.cfg.

Example 2:

We will now use the Install.cfg file from example 1 to temporarily grant the user "User" the right to change the floppy disk key on all workstations. In accordance with the pre-defined administration structures, this right is granted by the user "SUBADMIN". To achieve this, the SUBADMIN must generate a configuration file with the type "Change" and distribute this file to the appropriate workstations.

Procedure:

1. Run the configuration file wizard
2. Select configuration file type "Change".
3. Select "Install.cfg" as the base configuration file.
4. During authentication, logon to the configuration file with SUBADMIN (password: subadmin).
5. In the user settings, select these options:
   - In "USER" double-click "Rights".
   - Activate "Toggle floppy disk encryption"
6. Save as target folder "Change.cfg".
7. Distribute Change.cfg to user PC.

8.6 Changing frequently-used Registry settings with SafeGuard Easy's administrative template

To make the configuration procedure more user-friendly Utimaco has created its own administrative template for the group policy editor (Gpedit.msc). You can then use this template (file name: Sguard.adm) to make specific SafeGuard Easy settings quickly and conveniently without having to edit the Registry.

An Administrator can change the administrative template settings for a user PC either locally, via the group policy editor (Gpedit.msc), or centrally via group policy objects (GPOs) in an Active Directory environment. As a rule, users in an IT environment do not have administrator rights and therefore cannot change SafeGuard Easy policies themselves.

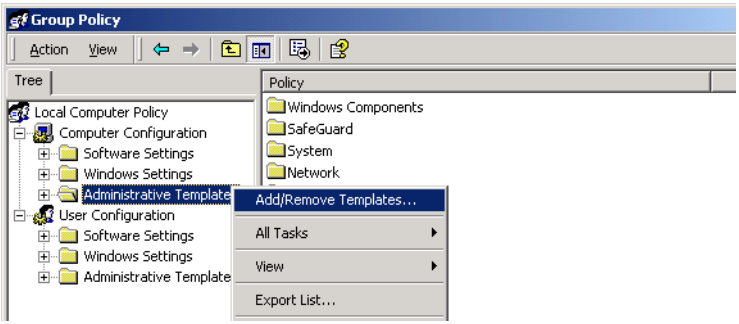
The next section briefly describes how to integrate an Utimaco template into a local system. Please refer to current Microsoft Documentation to find out how to use administrative templates in an Active Directory environment.

1. Log on as a user with Windows Administrator rights.

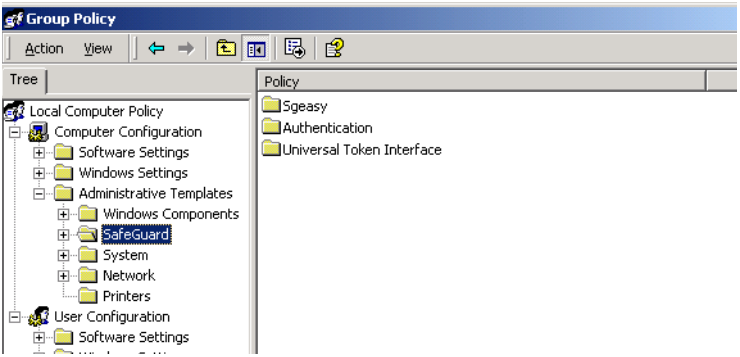
2. In Start / Run enter the command "gpedit.msc" and start the local group policy editor.

3. Add the SafeGuard template Sguard.adm via "Administrative templates" > "Insert templates".

Sguard.adm is stored in the SafeGuard Easy installation folder in the \ADM directory.



4. The "SafeGuard" folder appears next to the previous folders in the computer configuration.

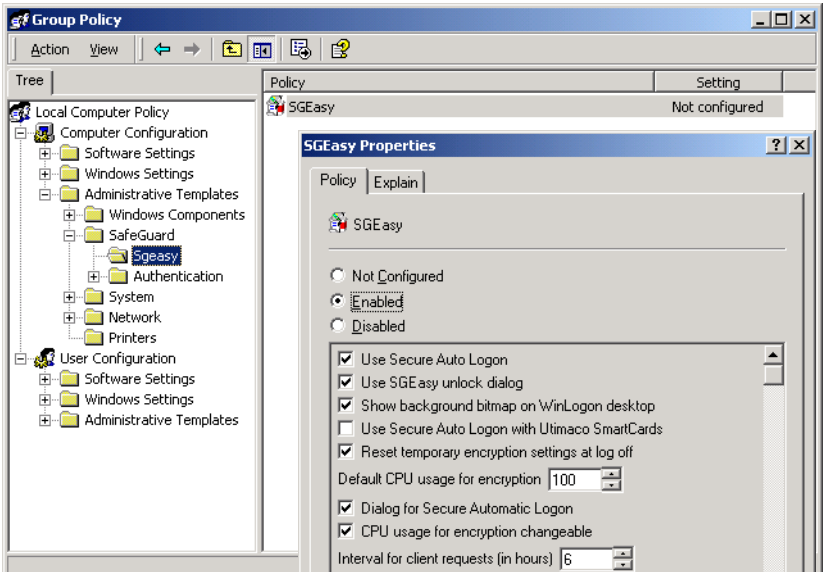


5. Non-Windows templates present a problem for this preconfigured view. As a result the following setting must be disabled for the individual policies view:

   Windows 2000:
   Mark "Administrative templates", select the "View" menu and deselect "Show policies only"

Windows XP/Windows Server 2003:
Mark the “Administrative templates” folder, select the “View” menu then "Filtering" and deselect "Only show policy settings that can be fully managed".

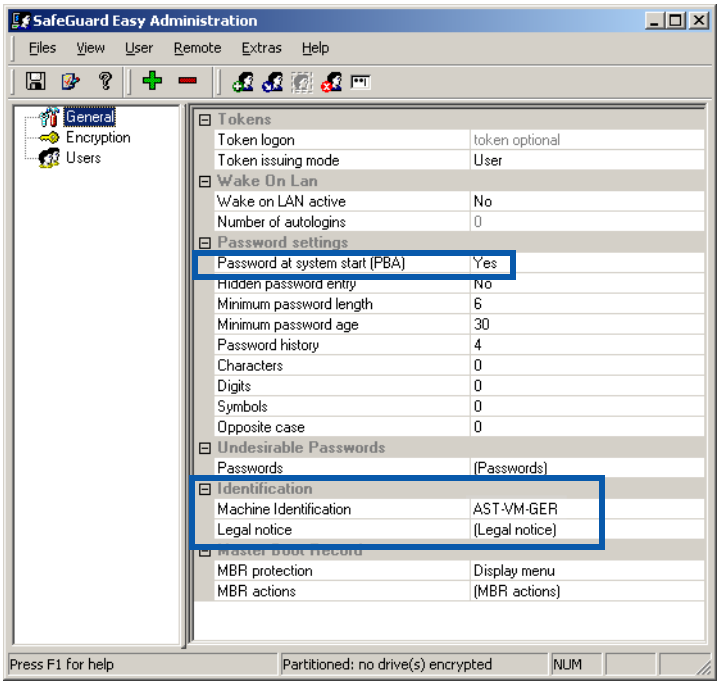
6. Double-click a policy to open it and make the settings for the features under “SGEasy Properties“.



Polices can have one of three different states:

- **Not Configured**
  The settings currently used by the user have not been changed i.e. previously-made settings are retained.
- **Enabled**
  The settings are transferred.
- **Disabled**
  The settings are removed.

9 Pre-Boot Authentication (PBA)



Pre-Boot Authentication (PBA) is a logon function that requires the user who is attempting to log on to authenticate themselves before the boot process. For more information on Pre-Boot Authentication, please read 'System boot and logon'.

You specify the PBA settings on the "General" configuration page.

9.1 Changing the language used in pre-boot authentication at a later point in time

The logon screen uses the language selected during installation (German, English or French), Users now no longer have to de-install SafeGuard Easy to display the pre-boot authentication texts in a different language.

> ***WARNING:***
> You can only change the texts displayed in the pre-boot authentication phase retrospectively: you cannot change the keyboard layout.

Parameters for changing the user interface language

You can call SetPBALang with these parameters:

```
SetPBALang [en | de | fr] | [n]
```

`[en | de | fr]`	Specifies the new language
`[n]`	Uses a number (1-255) for the language setting The following languages are supported: 9=English 7=German 12=French

After you restart the PC, the changed language setting applies.

You will find SetPBALang in the SafeGuard Easy program folder.

9.2 Switching on password at system start (PBA)

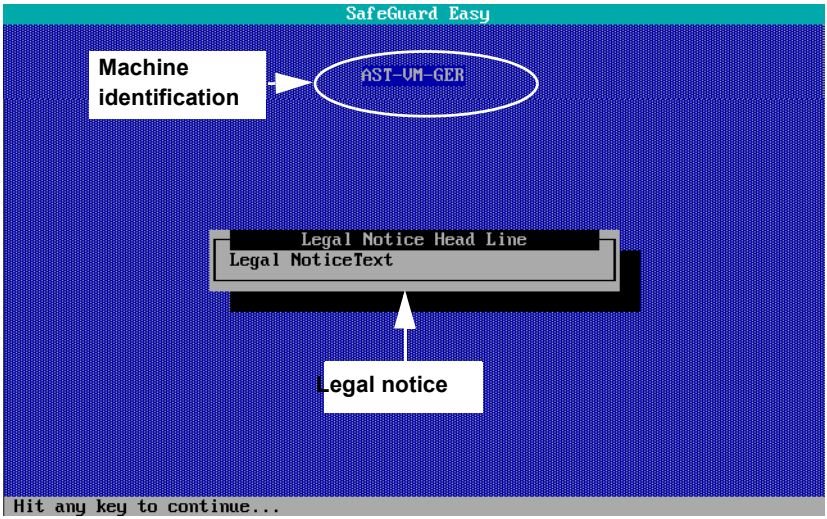
The "Password at system start" option switches Pre-Boot Authentication (PBA) on/off. If PBA is switched on, a logon screen is displayed before the operating system is loaded. Windows does not run until after successful authentication with the correct SafeGuard Easy access data.

If you switch off Pre-Boot Authentication, no logon is necessary before the system boots. Authentication then uses the familiar existing operating system functions.

For security reasons you should never deactivate Pre-Boot Authentication!

9.3 Machine identification

You can use the options in "Machine Identification" to display freely definable texts during PBA.



9.3.1 Machine identification

The text you enter here appears in the PBA logon screen. You can, for example, specify an exact name for your workstation in this field, which enables you to identify the machine precisely. If a machine name is already set in the Windows network settings, it is transferred automatically.

You can set a maximum of 63 characters.

The machine ID string can contain references to environment variables. These will be expanded at the time of installation. This is especially useful for configuration files that are installed on more than one computer.

Example:

The entry "*This is %USERDOMAIN% booting from %WINDIR%*"

will expand to "*This is PC1234 booting from C:\WINNT"*

during installation.

A special variable, %COMPUTERNAME%, is available on all operating systems to provide a non-platform-specific way of adding the computer name. %COMPUTERNAME% will always expand to the computer's NETBIOS name.

The following rules also apply:

- Undefined variables expand to an empty string.
- If the contents of a variable are too large to fit the machine ID field, it is expanded to "[...]".
- Variable names are not case sensitive.
- If you need a percentage sign in the string, use the character sequence "%%"
- Variable expansion is performed once during installation, not every time the computer is booted.

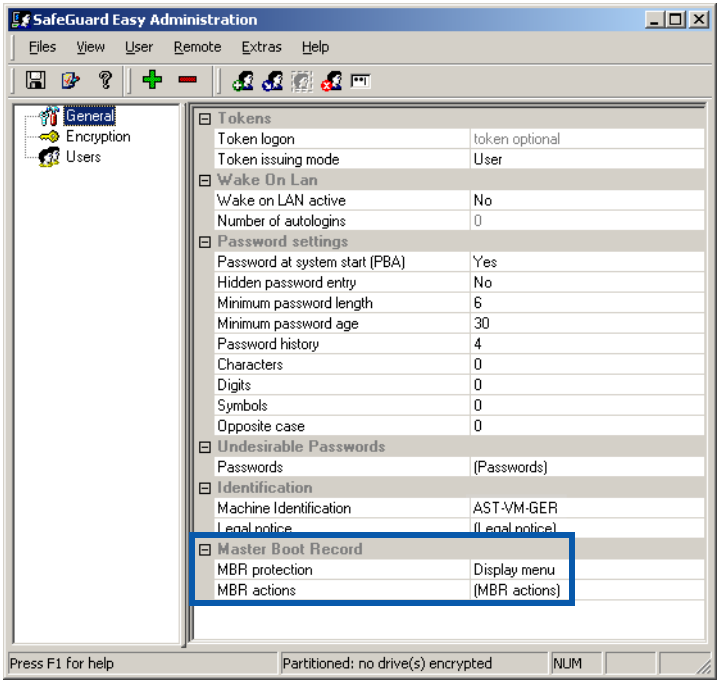
9.3.2 Legal notice

This is a text box whose contents you can define, and which are displayed in PBA **before the logon with the SafeGuard Easy data**. In some countries it is a legal requirement for a text field with particular contents to be displayed.

The title can contain up to 68 characters and the text block can contain up to 10 lines with 70 characters each.

The user must confirm the text box before the system continues booting.

10 Master Boot Record



The hard disk's Master Boot Record (MBR) stores a variety of information about all the partitions created on the hard disk. The system uses this information to find out which hard disk drive, and which partition, is used to boot the system. For this reason the MBR is a popular point of attack for viruses because the BIOS executes the machine code it contains right at the start of the booting process, before the operating system has been loaded. SafeGuard Easy can identify modifications to the MBR and respond to them in various ways, such as displaying a menu and letting the user select a specific action that will be performed after changes have been made.

You specify the MBR settings on the "General" configuration page.

10.1 MBR protection

The MBR protection function protects against viruses that attack the partition sector. If you have not selected "Ignore changes", the system checks the MBR for changes each time the system boots.

- **Ignore changes**

  No changes are made. The original MBR is not restored and the boot process continues without intervention.

- **Display menu**

  If the MBR has been changed, a menu is displayed in which you can select the following actions:

  - Default Action
  - Undo Changes
  - Ignore Changes
  - Keep Changes

  Select *Default Action* to run the "Default action". Select *Undo Changes* to restore the original status of the MBR from the internal backup. If you select *Ignore Changes*, no changes are made. If you select *Keep Changes* the current MBR is left unchanged but the internal backup is updated. The check takes place before the user logon. The menu only appears after a successful logon. This prevents an unauthorized user from specifying what should happen in such a case.

10.2 MBR default actions

You can select one or more default actions to check the MBR.

- **Display warning**
  The user is notified that the MBR created for SafeGuard Easy has been modified. The user must press a key to confirm this message.
- **Restore MBR**
  The original MBR is restored automatically as a backup copy without notifying the user. The system then reboots to remove any viruses that may be present.
- **Halt System**
  If the MBR has been changed, the system displays a message and halts after logon, if the user attempts to log on. (However, the system administrator can still logon.) It is now no longer possible for the user to boot the workstation, and the user is forced to request help from the administrator or support staff.

10.3 Support Compaq Setup partition

This option leaves the MBR virtually unchanged. This is necessary on certain Compaq Systems (and possibly on others too) to enable access to the setup partition. Click "On" to keep the original MBR. If you do not want to set this option, select "Off". This option can be selected with all encryption modes (Full disk encryption, Partitioned, Boot protection).

We recommend that you only select this option if it is necessary. If you do not know your system's reaction please contact Compaq's hotline.

11 Encryption

SafeGuard Easy's core task is to encrypt data on different data media such as hard disks, floppy drives and removable media drives.

The benefit of encrypting floppy and removable media drives is that all data communications with the outside world are encrypted. It is not possible to read plain text floppy disks on a PC where encryption is active. Unreadable floppy disks must be reformatted in the encrypted disk drive before they can be used. However, you will lose all the data during formatting! If floppy disks are exchanged between different workstations, the floppy drives on the workplaces concerned must be encrypted and deciphered with the same algorithm and key. If this does not happen, the floppy cannot be read.

Users with appropriate rights can temporarily change the key for floppy disks and removable media, provided that encryption is active (see 'Toggling floppy disk and device encryption').

It uses different keys for encryption, and implements different algorithms (AES-128, AES-256, Rijndael-256, IDEA, 3DES, DES, DES SB-II, Blowfish-8, Blowfish-16, STEALTH-40, XOR and XOR SB-I A=B). The key is encrypted after it has been defined and is not stored in the system, for security reasons. During the boot procedure, the key is regenerated each time from a code saved on the hard disk and the SafeGuard Easy password of the user.

You can decide to encrypt a maximum of four hard disks, or simply the system areas or individual partitions. The following file systems are supported: FAT-12, FAT-16, FAT-32, HPFS, NTFS and NTFS5. The number of partitions on a hard disk is limited to eight.

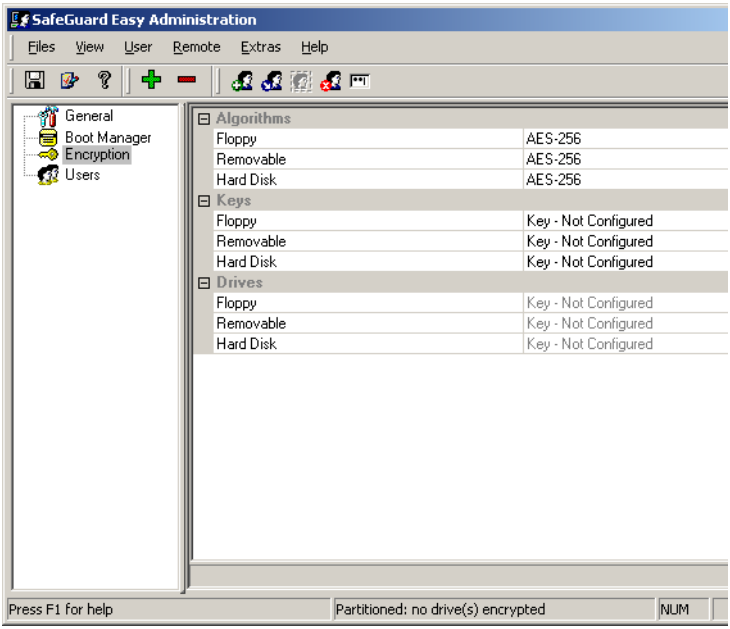
To fine-tune access protection on your system we recommend you use the following modules from the SafeGuard product family:

- **Application-Specific Access Rights (ASAR):**
  Implements a 3-dimensional security concept with which explicit rights can be specified between the users, data and applications. This provides protection against the threat posed by particular (even currently unknown) viruses and ensures a level of security, even in unmanaged code or heterogeneous Windows environments.

- **Plug and Play Management (PnP):**
  Users can connect any PnP devices, such as USB memory sticks, and use them immediately. PnP Management enables you to control data import/export on memory media at class level and for individual devices.

11.1 Configuring encryption

You specify the encryption settings on the "Encryption" configuration page in the administration programs.



11.2 Supported disk drives

Hard disks

- IDE/SCSI hard disks
- Serial ATA hard disks (hot-pluggable)
- Firewire hard disks (hot-pluggable)
- USB hard disks (hot-pluggable)

Information about hard disk encryption:

- **Hot-pluggable hard disks**

  All hard disks that are to be encrypted must already be connected to the PC before SafeGuard Easy is installed.

  Do not interrupt the initial encryption of hot-pluggable hard disks!

  The hot-pluggable hard disks must also still be connected during the first reboot after initial encryption. After initial encryption the disk drive can be connected and removed again as required, provided that the user always uses the same hard disk, for regular data backups, for example. There are usually no problems if they do so.

  Problems may arise if several hard disks are used (for example, an encrypted hard disk is removed and an unencrypted hard disk is then connected), such as corrupting the SafeGuard Easy encryption table.

  It is essential that the disk numbering (Disk Management) during operation is the same as the numbering used during the installation process or initial encryption.

The restrictions mentioned apply to Serial ATA hard disk drives only if they are used as hot pluggable hard disk drives.

- **Different hard disk types**
  If possible, avoid mixing different hard disk types (IDE/SCSI) on one system.

- **Unformatted areas**
  If no specific file system has been assigned to a partition, SafeGuard Easy will not recognize this partition in the case of installation type "Boot Protection", and the unformatted area of the hard disk will also remain encrypted.

- **Additional hard disks**
  SafeGuard Easy automatically recognizes whether your computer has one or more hard disks. After installing SafeGuard Easy, do not install additional hard disks in the system. If you want to install an additional hard disk in the system, you should first completely remove SafeGuard Easy. After removing, install the new hard disk and re-install the SafeGuard Easy program.

- **Re-partitioning**
  If a hard disk has been re-partitioned, you must restart the PC BEFORE installing SafeGuard Easy.

  After encryption, do not change the partitioning on the hard disk. This can lead to data loss.

- **Key**
  Only one hard disk key is defined, no matter how many hard disks there are.

- **System kernel backup**
  After hard disk encryption you absolutely must create a backup of the system kernel!

Floppies

- SafeGuard Easy supports any disk drive that is integrated in a standard PC.

Information about floppy encryption:

- **Boot floppy disk**
  If floppy disk encryption is activated, you should must create an encrypted boot floppy disk.
- **Several floppy disk drives**
  If more than one floppy drive is present, the different floppy drives are not displayed individually, but collectively ("A+B").Floppy disk drives cannot be encrypted individually. The encryption status applies to all floppy disk drives.

Removable media

- USB memory stick
- Memory card in integrated reader slot (SD card, CF card etc.)
- Lenovo Microdrive
- USB ZIP disk drive
- Parallel ZIP disk drive

Information about removable media encryption:

- **Connection possible after installation**
  Removable media must not be connected when SafeGuard Easy is being installed (but exceptions are possible if, for example, a USB memory stick does not work with the standard Microsoft driver, but requires its own driver).

- **Initial encryption**
  Removable media are not "initially encrypted": they are formatted as soon as encryption is switched on (at all times after the installation of SafeGuard Easy).

- **SG Eject**
  Removable media drives are handled like hard disks, provided no suitable software provided by the disk drive's manufacturer is used. If a removable media drive is encrypted, only users with Windows administrator rights can eject a removable medium. Users without administrator rights must use SG Eject. You will find SG Eject in the context menu for the drive.

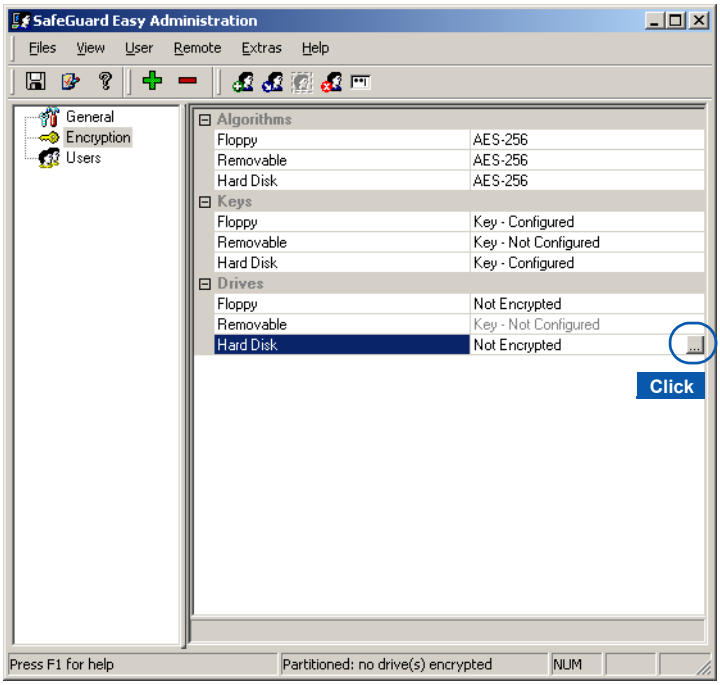
11.2.1 Encrypting disk drives

The example below involves hard disk encryption, but the procedure is identical for floppy and removable media drives:

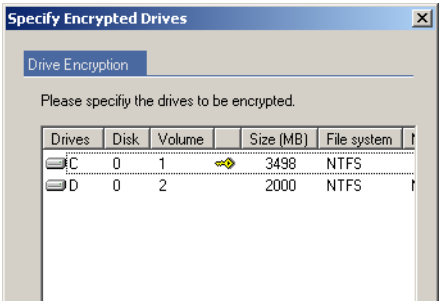
1. Select an algorithm for the hard disk drive.

2. Define a key.

3. Under "Drives", click "Hard disk".



4. You see a dialog called *Specify Encrypted Drives.*



   If you now double-click a drive letter, you see a key icon. This shows that the disk drive/ partition is now encrypted.

   Which hard disks/how many partitions are (or can be) encrypted depends on the configured encryption mode. The encryption mode (see 'Encryption mode') for a workstation is set during installation, or when a configuration file with the attribute "Install" is generated, and you cannot change it later.

5. If you want to switch off encryption, double-click the drive letter again. The key icon disappears and encryption is deactivated for that drive.

11.3 Keys

Only a user who has the correct key can access encrypted disk drives. A key consists of a sequence of characters (numbers, letters, particular special characters), and it is also subject to specific rules, like a password.

A disk drive key must be assigned before initial encryption. For each drive you can either define a key yourself or have one generated by the system.

11.3.1 Key management

The SafeGuard Easy key management function stores keys securely. All the keys are stored in an encrypted area of the SafeGuard Easy system kernel, and enciphered with an encryption key (known as the "KEK", from **K**ey **E**ncryption **K**ey). The KEK itself is not stored on the hard disk, but is generated from the SafeGuard Easy password.

11.3.2 Creating keys

The keys cannot be created without the correct SafeGuard Easy password and, as a result, the data on the hard disk, floppy disk or removable media is not accessible.

If PBA is switched on: The keys for decrypting the disk drives are only generated if the correct SafeGuard Easy data is entered during PBA.

If PBA is switched off: The keys are one-way encrypted and saved on the hard disk. Despite this, encryption and key management are absolutely identical to the selection "PBA switched on". On the other hand, they handle the password (or the scan code) in different ways: during PBA, instead of waiting for a user to enter the user name and password manually, SafeGuard Easy has this data to use. To arrange this, whenever PBA is switched off, SafeGuard Easy always creates a user called "*AUTOUSER" and creates a random password for this user. This password is split into different parts and stored in the SafeGuard Easy kernel. During the boot procedure SafeGuard Easy can recover the complete password (or actually the complete scan code sequence) from this stored password.

11.3.3 Key length

There is no pre-defined minimum key length. The maximum key length is 32 characters (ASCII code 32 to 255). Alphanumerical characters (A-Z; a-z; 0-9) and special characters (°!"„§$%&/()=?´*'-:;^+#-.,) can be used for the key, with the exception of country-specific special characters. Note that the system differentiates between upper case (e.g. A) and lower case letters (e.g. a).

11.3.4 Trivial keys

Keys for floppy disks, hard disks and removable media are checked for "triviality". A trivial key uses character strings consisting of one or a few characters (for example, 22222222, aad daad daadd, 1h1h1h1h1h1h1h) or the sequence of keys on a keyboard (for example, asdfghjk, lkjhgfds). If a trivial key is found, a message warns you about the security risk and you can define a new key.

11.3.5 Random keys

A random key always has the length 32 bytes (256 bits). It is then reduced to the length suitable for the selected algorithm. The * characters in the input field for the key act only as placeholders.

We strongly recommend that you generate a random key for hard disks or partitions is when SafeGuard Easy is installed on several workstations with only one configuration file: in this way, although the same configuration settings are used on each computer, different, non-trivial random keys are generated.

If floppy disks/removable media are regularly exchanged, for example between members of staff, the keys should **never** be generated by random. Media enciphered with a random key can only be read on the workstation on which they were encrypted.

11.3.6 Defining keys

By default, only the system administrator (SYSTEM) can enter all keys. Other users must be assigned the appropriate right so that they can also enter keys. Keys for hard disks, floppy disks and removable media can be different. On all disk drives, in contrast, only one key can be assigned.

To assign a key for the first time, or change a key, select the "Key" menu item. You enter the key in the same way for all disk drives, and the same key rules also apply. When you have entered the key, or selected a random key, click the [OK] button to confirm.

Never tell unauthorized outsiders a custom key!

11.3.7 Changing a key

Encrypted hard disks or partitions must first be decrypted before you can assign a new key.

A new key for floppies and removable media can be set at any time, either by the SYSTEM SafeGuard Easy user or by a user who has the appropriate rights. However, please note that this will mean you will no longer be ably to read any media that were encrypted with the "old" key. Users can only access the "old" media if they have authorization to change the floppy/removable media key (see 'Toggling floppy disk and device encryption').

11.4 Algorithms

The different algorithms are assessed, especially, on the basis of the level of security they provide. It is usually true that, the more secure a procedure is, the longer the encryption process takes.

11.4.1 Selecting an algorithm

To select an algorithm, go to *Algorithms* and click a disk drive. Then select an algorithm for that disk drive from the pull-down menu. By default, the **AES-256** algorithm is selected automatically.

11.4.2 SafeGuard Easy algorithms

Below you will find a list of all algorithms that can be used in SafeGuard Easy, along with their particular standards:

Algorithm	Key lengths
AES-256	32 bytes (256 bits)
AES-128	16 bytes (128 bits)
Rijndael-256	32 bytes (256 bits)
DES	7 bytes (56 bits)
3DES	21 bytes (168 bits)
IDEA	16 bytes (128 bits)
Blowfish-8	32 bytes (256 bits)
Blowfish-16	32 bytes (256 bits)
STEALTH-40	5 bytes (40 bits)
XOR	8 bytes (64 bits)

AES-128
The Advanced Encryption Standard (AES) is a new algorithm that replaces the Data Encryption Standard (DES). The Rijndael algorithm was selected for AES by the American National Institute for Standards and Technology. AES is a very fast, secure encryption algorithm and works with a 128-bit key.

AES-256
AES-256 is the same as AES-128, but uses a 256-bit key and 128-bit block length.

Rijndael
Rijndael is a special implementation of the AES 128-bit algorithm but works with a 256-bit key and a 256-bit block length.

IDEA (International Data Encryption Algorithm)
This symmetrical encryption algorithm, developed at the beginning of the 1990s, works with a 128-bit key. Nowadays it is considered very secure, due to the mathematical process involved, and its key length, and it is considered extremely resistant to all crypto-analytical attacks. If you want to install a highly-secure system, we recommend you use IDEA.

DES (Data Encryption Standard)
DES was developed in the 1970s and works with a 56-bit key.

3DES (Triple DES)
Triple DES, or 3DES for short, is a further development of the Data Encryption Standard (DES). 3DES uses three sequential encryption runs of the DES algorithm and operates with a 168-bit-key. The 3DES procedure is very secure but rather slow.

Blowfish-16/Blowfish-8
Blowfish is a symmetrical algorithm. It uses a 64-bit block coding algorithm and a 256-bit key.

Blowfish-8 is the same as the Blowfish-16 algorithm, but reduced to 8 rounds and uses a 256-bit key.

STEALTH-40
The STEALTH algorithm uses a 40-bit key.

XOR (eXclusive Or opeRation)
XOR is a symmetrical algorithm. However, its security level should be regarded as low. XOR uses a 64-bit key.

Tip: If you want to set up a high-security system, we recommend you use IDEA or AES/Rijndael.

Special floppy drive algorithms:

- **DES SB-II**

  The DES SB-II algorithm is compatible with the floppy drive coding of SafeBoard II and III and/or the floppy drive encryption of SafeBoard X II and II with the old key management.

- **XOR SB-I A=B**

  See XOR properties. XOR SB-I A=B is compatible with floppy drive encryption from SafeBoard I (from Version 1.43), C:Crypt and Crypton DOS.

11.4.3 Changing an algorithm

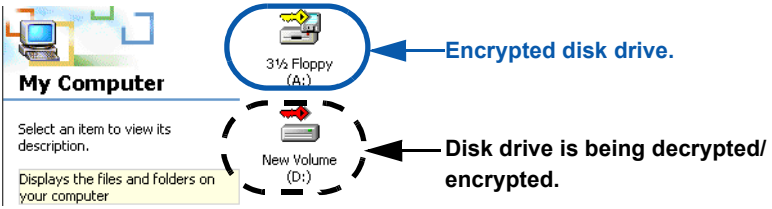
After SafeGuard Easy has been installed you can no longer change the selected algorithms. To select a different algorithm you must re-install SafeGuard Easy.

11.5 Displaying encryption status in Windows Explorer

The encryption status of the disk drives is indicated with a colored key in Windows Explorer.

Yellow key means that a disk drive is encrypted.

Red key means that an encrypted disk drive has just been decrypted (or vice versa).


My Computer
Select an item to view its description.
Displays the files and folders on your computer
3½ Floppy (A:)
New Volume (D:)
Encrypted disk drive.
Disk drive is being decrypted/ encrypted.

11.6 Creating an image of an encrypted hard disk drive

Imaging tools like Symantec Ghost are used for the fast, automated initial installation of a large number of PCs, for example if a major insurance company wants to set up 10,000 notebooks identically using imaging software such as Symantec Ghost. Imaging tools can also repair corrupt partitions, if, for example, corrupt partitions are repaired by restoring an image file from the network or a CD.

In general, creating images of encrypted hard disk drives (partitions) may cause problems.

The main reasons for this are:

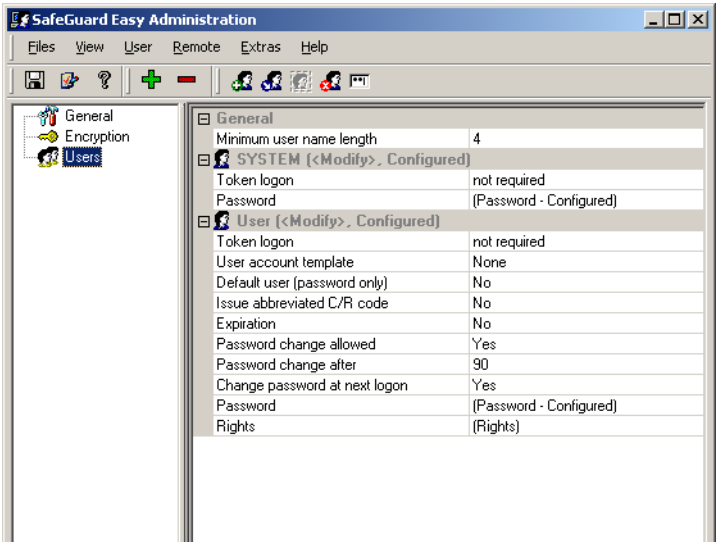
- Encrypted data cannot be compressed so that the image file will be the same size as a hard disk (e.g. 40GB)!
- The partition size should not be changed. If it is, it will not be possible to restore the Image.
- After cloning a hard disk drive that is protected by SafeGuard Easy all the encryption keys created by SafeGuard Easy will be the same on every machine.

Imaging software (for example Symantec's Norton Ghost) can also be used to backup and restore partitions to a SafeGuard Easy encrypted hard disk. The imaging tool must be able to decrypt the encrypted partition.

You will find more information on this subject in the Utimaco Knowledge Database http://www.utimaco.com/myutimaco.

Use the Knowledge database's "Search" field to look for key words like "Image" or "Imaging".

12 Creating user profiles



In this area you specify which users can work at a workstation that has been protected with SafeGuard Easy. Here you can create new SafeGuard Easy users, change existing users, or delete users that are no longer required. In addition you specify which additional properties and rights the defined SafeGuard Easy users have.

SafeGuard Easy allows a maximum of 16 users (including *AUTOUSER) to have access to the system. The defaults are SYSTEM and USER, of which the SYSTEM user can never be deleted.

NOTE:
The Configuration File Wizard only shows SYSTEM and USER if a file with the attribute "Install" has been generated, or used as a base configuration.

12.1 Defining admin tasks

In SafeGuard Easy, users with admin tasks and users without admin tasks are handled differently.

Users with admin tasks include the

- system administrator and
- users with administration functions.

The person without admin tasks is the

- user

The administration function can be kept separate from the user function, or not, as required. The admin tasks can be carried out by one or more people. SafeGuard Easy can be configured for at least one user, and a maximum of 16 users (including *AUTOUSER).

However, depending on the needs of your organization, it may be sensible to create a multi-level roles system in which the system or sub-system administrator are granted different hierarchical rights. The following hierarchical structure is possible:

System administrator

Only the system administrator can perform all program functions. They can define a deputy and assign them particular admin rights. The system administrator must never forgot their password. They should write it down and save it in a safe place.

Sub-system administrator

Sub-system administrators can help the user if, for example, they have forgotten their password. The extent to which a sub-system administrator can support the system administrator in their work depends on the sub-system administrator's pre-defined rights.

Users

The user can only see their settings in read-only mode. By default, they can only run the function for changing their user password. In addition, the system administrator can assign the user different rights.

12.2 Pre-defined users

During installation, SafeGuard Easy automatically creates profiles for the following users:

- SYSTEM
- USER
- *AUTOUSER

12.2.1 The SYSTEM user

This user has the highest hierarchy level, which they do not share with any other user. Even the SYSTEM user cannot change their own settings. The SYSTEM user data cannot be deleted by anyone, and cannot be administered by anyone. The SYSTEM user is the only one who can change the settings of all other user profiles. For this reason, only the top-level system security officer should be able to log on with the user name SYSTEM. In addition, only the top-level system security officer should know the password for the SYSTEM user. They should write it down and leave it in a secure place such as a safe.

12.2.2 The USER user

Like the SYSTEM user, the user USER is automatically present after SafeGuard Easy has been installed. This user profile has no rights and can be deleted at any time.

12.2.3 The *AUTOUSER

The *AUTOUSER is a special feature. Whenever PBA is switched off, SafeGuard Easy always creates a user called "*AUTOUSER" and creates a random password for them. This password is split into different parts and stored in the SafeGuard Easy kernel. During the boot procedure SafeGuard Easy can recover the complete password from this stored password, and carry out the logon.

By default the *AUTOUSER has no rights. They can be granted the following rights:

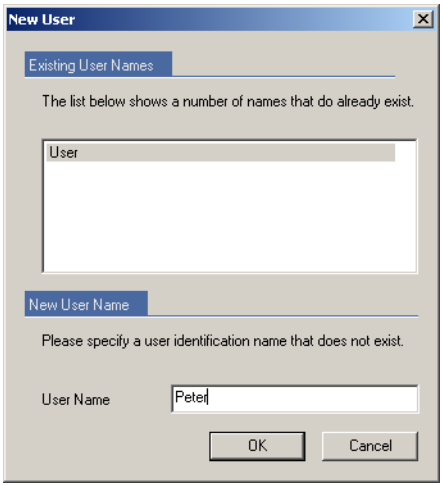
- Change device keys temporarily
- Change floppy keys temporarily
- Toggle floppy drive encryption
- Toggle removable media drive encryption

If PBA is switched off, all users log on with the *AUTOUSER's profile. If PBA is activated again, the *AUTOUSER is automatically deleted.

12.3 Creating users

You create a new user profile in the administration programs, in the "Users" configuration page.

After clicking the "Create User" icon you see the *New User* dialog.

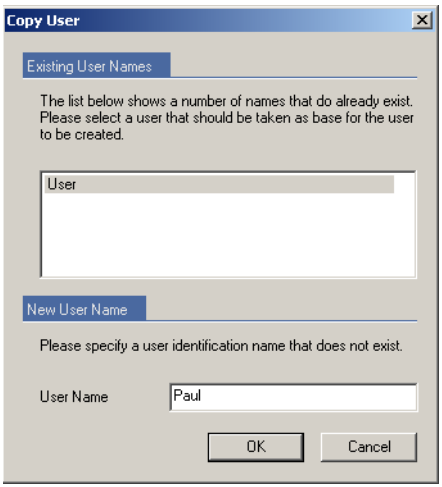


Give the new user a name by entering it in the text field. The new user name must not be more than **16 characters** long. If the name has already been assigned, an error message appears. By default the new profile has no rights. For more information about assigning rights, see Rights.

12.4 Copying a user

You can copy user profiles that are similar, and then change them if required. This procedure saves time.

After clicking the "Copy User" icon you see the *Copy User* dialog.


Copy User
Existing User Names
The list below shows a number of names that do already exist. Please select a user that should be taken as base for the user to be created.
User
New User Name
Please specify a user identification name that does not exist.
User Name
Paul
OK
Cancel

In the profile, select the existing profile that you want to copy. All profiles in your area of administration are displayed. However you can only copy profiles that are at a lower hierarchy level than your own profile.

The SYSTEM user cannot be copied.

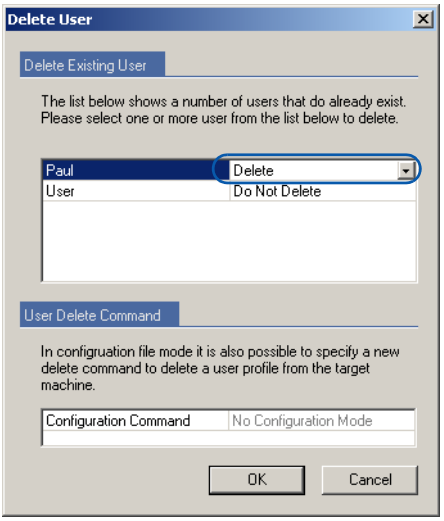
Give the new user a name and click [OK] to confirm your entry is correct. If the name has already been assigned, an error message appears.

After this you can change the new profile if required.

12.5 Deleting users

You can delete user profiles that are no longer required.

After you clicking the "Delete user" icon you see the *Delete User* dialog.


Delete User
Delete Existing User
The list below shows a number of users that do already exist. Please select one or more user from the list below to delete.
Paul
Delete
User
Do Not Delete
User Delete Command
In configuration file mode it is also possible to specify a new delete command to delete a user profile from the target machine.
Configuration Command
No Configuration Mode
OK
Cancel

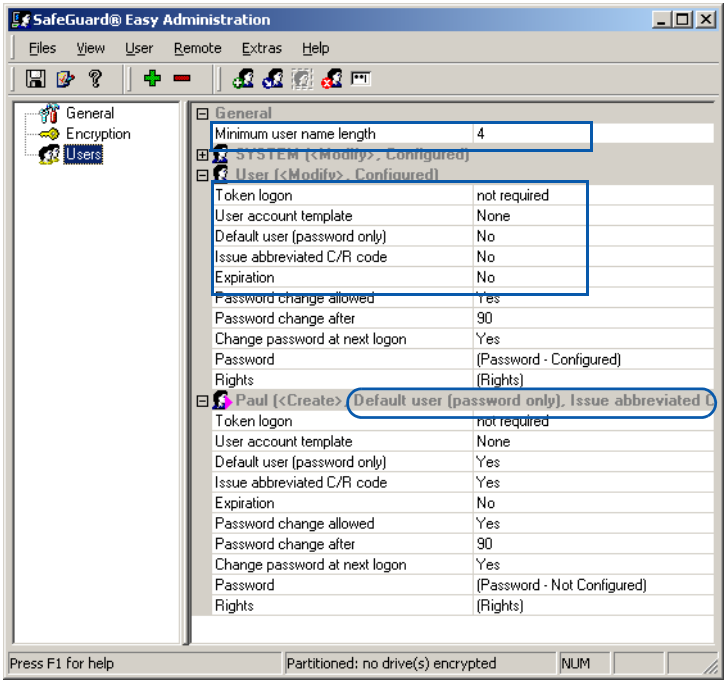
In the user list, select the existing user profile you want to delete. All profiles in your area of administration are displayed. Click the pull-down menu next to the user names and assign the attribute "Delete" to the relevant user name.

You can only delete profiles that are at a lower hierarchy level than your own profile.

You cannot undo the deletion of a user.

12.6 User features

The features assigned to a user are shown by the extensions after the user name.



12.6.1 Minimum user name length

You define the minimum length of a SafeGuard Easy user name (number of characters). You can either type in the number of characters, or increase or decrease it by pressing the direction keys. You can enter any value between 1 and 16.

12.6.2 Token logon

This setting specifies whether a user must log on with a token or not. This option can only be selected if token support was installed with the option "Optional" during installation. For details of Token support, please read 'Token support'.

12.6.3 Default user (password only)

One single SafeGuard Easy user can be set as a default user - except the SYSTEM user. To log on, a default user only enters the SafeGuard Easy password. If other users besides the default user want to log onto the workstation, they must activate "Extended logon" (during PBA, by pressing [F2]).

12.6.4 Issue abbreviated C/R Code

This function is particularly suitable for sub-system administrators who are responsible for remote administration.

This property influences the length of the response code that is exchanged during a Challenge/Response procedure.

Users with the "Issue abbreviated C/R Code" property (and the SYSTEM user) generate short response codes that have only 30 characters, whereas "normal" SafeGuard Easy users generate response codes that are 56 characters long. When these are typed in or passed on to the user, this can lead to increased errors.

For details of the Challenge/Response procedure, please read Chapter 'Remote Administration'.

12.6.5 User account template

Templates serve a very special purpose and should only be used for that purpose. They are usually needed when SafeGuard Easy is to be installed on several computers with the help of a configuration file. If there were no templates, every user would have the same SafeGuard Easy user name on every computer. In many cases, however, this would contradict corporate organizational guidelines which stipulate that there must be individual user names, such as surnames, personnel numbers, etc. In this situation, a SafeGuard Easy user name can be defined as a template for this type of environment. When a template is used, this SafeGuard Easy user is assigned a new user name when they log on to PBA for the first time, so they are individualized.

A template is implemented as follows:

SafeGuard Easy is installed on a workstation and one SafeGuard Easy user is defined as a template user. This workstation's user is informed of the access data (user name and password) for the user template. When the user logs on for the first time, they must enter this access data in the logon screen. They are then requested to enter their new SafeGuard Easy user name and a new password, which they must also use for identification at their next logon.

A template can either be used to rename or copy a user.

Renaming a user

If you want to ensure that only one user can log on by using the template, you must assign the "Rename" attribute to the user template. If you do, the template is overwritten with the new user data, and it is no longer possible to log on with the template's access data.

Copying a user

The new user name is added to the list of SafeGuard Easy users but the user template remains unchanged. Other users can log on with the template's access data. A maximum of 13 new users can be added, when SYSTEM and USER are already on the workstation.
For security reasons we recommend that you use the "Rename" template.

12.6.6 Expiration date

The expiration date specifies the maximum period of validity for a SafeGuard Easy user profile. You can set a deadline date or time period at which the user can log on to the system for the last time. You can simply type in the date or a particular period in time.

This setting is especially suitable if, for example, staff such as temporary staff or students on work experience are only intended to use a workstation for a particular time period. After the pre-defined deadline has passed, the workstation is blocked for the user.

This setting has no validity for the SYSTEM user.

12.7 User rights

You need to decide which access rights are to be assigned to the individual SafeGuard Easy users. For security reasons this needs careful consideration.

You can assign users rights for temporary and permanent settings. Temporary settings are settings that only apply for the duration of one work session. When the computer restarts, the temporary settings are no longer valid and the system settings are applied again. Permanent settings are settings that still apply after the computer restarts.

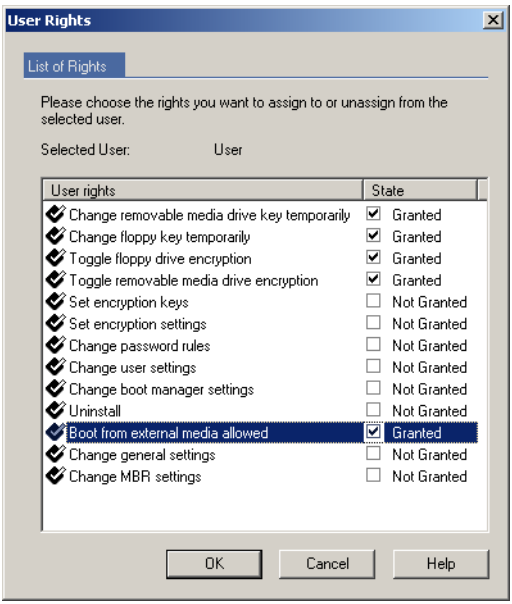
You can assign the following rights:

Change removable media key temporarily	Permits the user to change the key for the removable media drives during one working session.
Change floppy drive key temporarily	Permits the user to change the key for the floppy disk drives during one working session.
Toggle floppy drive encryption	Permits the user to switch floppy disk encryption on or off.
Toggle removable media drive encryption	Permits the user to switch removable media drives encryption on or off.
Change encryption key	Permits the user to change the keys for all drives. This does not apply to the hard disk if it is encrypted.
Change encryption settings	Permits the user to change the encryption state and the keys.
Change password rules	Permits the user to change all general password rules.

Change user settings	Permits the user to change all user settings. Must be set before other users can be assigned rights!
Change Boot Manager settings	Permits the user to change all Boot Manager settings.
Uninstall	Permits the user to remove SafeGuard Easy.
Boot from external media allowed	Permits a system protected with SafeGuard Easy to boot from external media such as floppies or CDs.
Change general settings	Allows changes to the following general settings: - Token - Wake-On-LAN - Change password on system boot - Hidden password entry - Identification
Change MBR settings	Allows changes to all settings for the master boot record.

12.7.1 Assigning user rights

If you double-click "User Rights", you see all the rights that can be assigned. If you double-click a right, its status toggles to "Granted" or "Not Granted" depending on its previous setting.



Initially, all new users have no rights. Only the SYSTEM user has all rights. Rights that the user is not authorized to change are not displayed in the view and cannot be changed or edited.

12.7.2 Transferring user rights

A user can also transfer their own rights (and only those rights) to another user. If an administrator (for example, a sub-system administrator) would like to change their own rights, they cannot do so themselves. They must ask an administrator who is more senior in the hierarchy (for example, a system administrator) to make the required changes.

To transfer their own rights to other users, the user must have a user profile with the right "Change user settings".

13 Password settings

The password plays a central role in SafeGuard Easy: the SafeGuard Easy password entered during Pre-Boot Authentication is used to generate the key needed to decrypt an encrypted hard disk, for booting.

You should choose your SafeGuard Easy password carefully. Users often tend to use the same passwords, or trivial passwords, such as their first or last names, company names, sequences of letters or numbers, etc. If a SafeGuard Easy password is too obvious it makes it easier for unauthorized outsiders to access a workstation. Careful consideration is needed to agree the strategy for defining how consistently password restrictions are to be applied, and they should also be tested before being implemented.

13.1 Pre-defined password rules

For security reasons SafeGuard Easy predefines several rules for all user passwords.

A SafeGuard Easy password can

- have a maximum number of 16 characters.

A SafeGuard Easy password is rejected, if it

- more than 50% of it consists of the same character (for example "aaabba", "222122").
- contains characters in sequence (for example "abcdef", "1234567").
- contains keyboard rows (for example "asdfghj").
- is identical to the SafeGuard Easy user name (except password for user "SYSTEM").
- is significantly similar to the SafeGuard Easy user name (except password for user "SYSTEM").
- is significantly similar to the previous password.

"Significantly similar" in this context means that the character sequence of the new password differs in at least 20% from the character sequence of the user name/old password. For example, the SafeGuard Easy user "USER" is allowed to use the password "U2SER13“, "U345SER" etc., but SafeGuard Easy does not accept passwords like "USER1", "USER2", "USERab", "12USER", "1USERF" etc.

13.2 Permitted keys for the SafeGuard Easy password

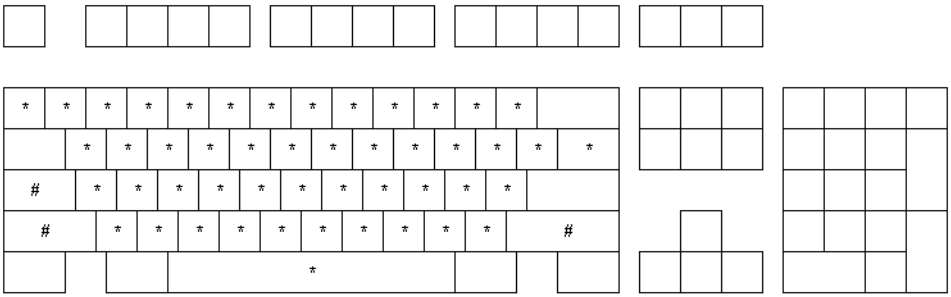
The SafeGuard Easy password can consist of a mixture of alphanumeric characters and punctuation marks.

SafeGuard Easy accepts

- all the keys marked with "*" in the figure.
- The [Shift] key and [Caps Lock] key (marked with "#" in the figure).

SafeGuard Easy does not accept

- the [Shift] key, if the [Caps Lock] key is already pressed.
- the [Alt] key
- the [Ctrl] key
- the Num number keys
- the F keys (for example, F1, F2)
- the direction keys

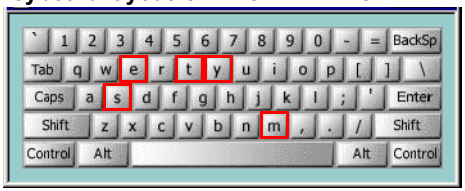


13.3 Configuring SafeGuard Easy for use in international environments

SafeGuard Easy stores all character strings in "scan code" form since, usually, no keyboard drivers are loaded in the Pre-Boot phase. The scan code is a code number (hexadecimal scan code) which the keyboard returns to the PC when a key is pressed. This code is independent of which letters, numbers or symbols are mapped to the key. It is a special identifier for the key itself, and is always the same for a particular key.

13.3.1 The effects of different keyboard layouts

As SafeGuard Easy stores all the character strings in "scan code" form, the scan code sequence for example for the password "system" on a **US keyboard layout** is: 1f-15-1f-14-12-32.

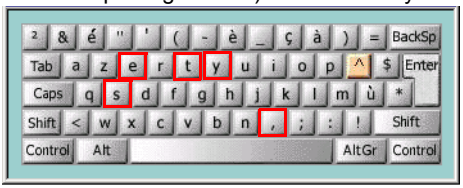


The scan code sequence for "system" on a **German keyboard layout** is: 1f-**2d**-1f-14-12-32.

> ***NOTE:***
> Y and Z are swapped round! A German-language user would therefore have to enter "szstem" to successfully authenticate themselves!

The password "system" on a **French keyboard layout** produces yet another scan code: 1f-**15**-1f-14-12-**27**.

A French-language user would therefore have to enter "syste," (note the comma replacing the "m") to successfully authenticate themselves.



You will find other keyboard layouts at http://www.microsoft.com/globaldev/reference/keyboards.mspx.

13.3.2 Generating internationally uniform data for SafeGuard Easy

If SafeGuard Easy is implemented in international environments, it is necessary to ensure that passwords and keys can be correctly entered (typed by the user) on all available keyboards. It is especially important to ensure that the SafeGuard Easy user profiles for performing administrative tasks can be implemented world-wide.

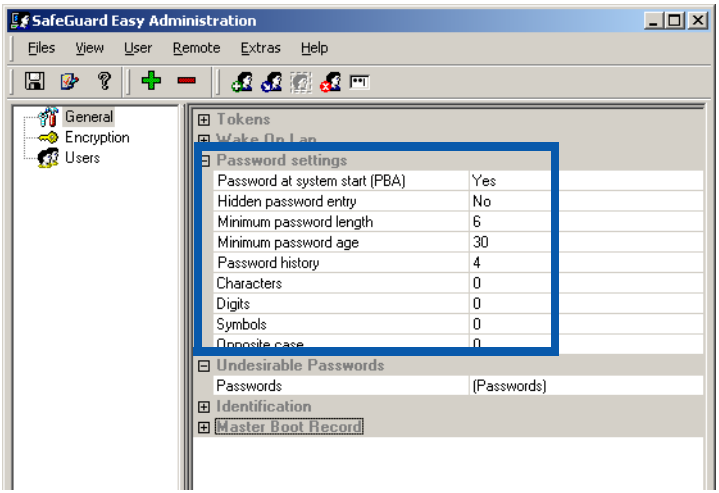
An example is the Challenge/Response procedure, if the user making the call and the help desk person using the Response Code Wizard do not use a keyboard with the same layout.

If the SafeGuard Easy data (or, to put it more clearly, keystroke sequence) is created from a combination of the following 21 keys, it is very likely that SafeGuard Easy can be used without problems in international environments.

Printed values on the keys	Hexadecimal scan code
b	30
c	2E
d	20
e	12
f	21
g	22
h	23
i	17
j	24
k	25
l	26
n	31
o	18
p	19
r	13
s	1F
t	14
u	16
x	2D
v	2F
[blank space]	39

13.4 General password rules

You can use the General Password Settings to define further rules for the formation of SafeGuard Easy passwords, such as the proportion of letters and numbers or their minimum length. These specifications apply to each SafeGuard Easy user, and no passwords are accepted that do not comply with these standards.



13.4.1 Password at system start

See “Pre-Boot Authentication (PBA)”.

13.4.2 Hidden password entry

Hidden password entry means that, in contrast to conventional logon procedures, no placeholders (e.g. the "*" character) appear when the password is entered. This means, for instance, that other people cannot see the number of characters entered. Cursor movement is also deactivated.
Please tell your users that characters are not displayed in the logon screen. Otherwise misunderstandings may occur if no "*" characters appear.

13.4.3 Minimum password length

You specify the password length in this field. In doing so you define the minimum length of a password (number of characters) when it is entered by the user.

You can either type in the number of characters, or increase or decrease it by pressing the direction keys. You can enter any value between 1 and 16 for the password length. The default value is 6 characters.

13.4.4 Minimum password age

The password age sets a minimum period of validity in days. During this time period the user cannot change the password. This option prevents the user from resetting the original password.

13.4.5 Password history

To prevent the user from constantly changing between a small number of passwords you can set the number of password generations to be higher. Each password is compared with the ones used in the past and rejected if it matches an old password. This setting controls how many passwords, that were used in the past, are saved for comparison.

The maximum number of used passwords that can be saved is 16. After clicking in the input field you can set the value, either by typing it or by clicking on the direction keys. It is especially useful to specify a number of password generations in combination with the setting "Change password after "n" days" ('Password change after').

Example:

The number of password generations has been set to 4 for the user Miller, and the number of days after which the user must change their password has been set to 30. Until now, the user Miller has logged on using the SafeGuard Easy password *"Computing". After the period has expired,* Miller is prompted to change their password in the SafeGuard Easy logon screen during PBA. User Miller types "Computing" in again, and sees an error message that this password has already been used, and they must choose a different password. User Miller cannot reuse "Computing" again until after the fourth prompt to enter a new password (since Password Generations has been set to 4).

13.4.6 Syntax rules (characters, digits, symbols, opposite case)

To increase the effectiveness of passwords you can require a mixture of letters and numbers (and/or symbols). The number entered is always a **minimum value**.

Symbols are special characters such as * # !"§$%&/() etc.

Opposite Case means that exactly the specified number of capital letters and lower case letters must be used in the password.

Example:

The **example** below shows the correct usage of syntax rules:

Settings

Letters: 1
Numbers: 2
Symbols: 1
Opposite case: 2

Result:

- AAaa12# is allowed
- aaAA123## is allowed
- 3456## is rejected
- AAB1# is rejected

Existing user passwords still apply, even if they not longer meet the specifications. The rules only take effect if the user changes their password.

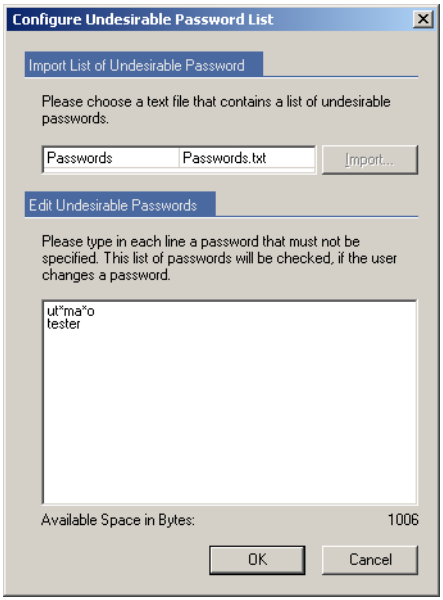
13.5 Forbidden passwords

You can use the Forbidden Passwords setting to define particular character strings that cannot be used in SafeGuard Easy passwords. Every new password is compared against the list and only accepted if it is not present in the list.

You can import an existing list or enter forbidden passwords yourself.

13.5.1 Defining forbidden passwords

Double-click "Passwords". In the "Edit Undesirable Passwords" text box, enter character combinations that are not permitted, separating them with [Ctrl] + [Enter].


Configure Undesirable Password List
Import List of Undesirable Password
Please choose a text file that contains a list of undesirable passwords.
Passwords
Passwords.txt
Import...
Edit Undesirable Passwords
Please type in each line a password that must not be specified. This list of passwords will be checked, if the user changes a password.
ut*ma*o
tester
Available Space in Bytes:
1006
OK
Cancel

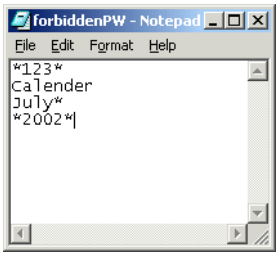
Enter trivial passwords such as test, system, user etc. in the list. Each password which is significantly similar to the forbidden password will be rejected. "Significantly similar" in this context means that the character sequence of the password must differ in at least 20% from the character sequence of the forbidden password. For example, if "tester" is on the list the password "tester1234" is allowed whereas "tester12" is forbidden.

You can also use wildcards to define trivial passwords. The only accepted wildcard character is "*" (asterisk). This means that, at the position indicated by the character "*", the password can contain **one** different character. For example, if you enter "ut*ma*o", any password like "utimaco", "ut1ma2o" is forbidden.

WARNING:
If you only enter the wildcard, or a large enough number of jokers, in the list of forbidden passwords, users will be unable to log on to the system again after being forced to change their password.

13.5.2 Importing a password list

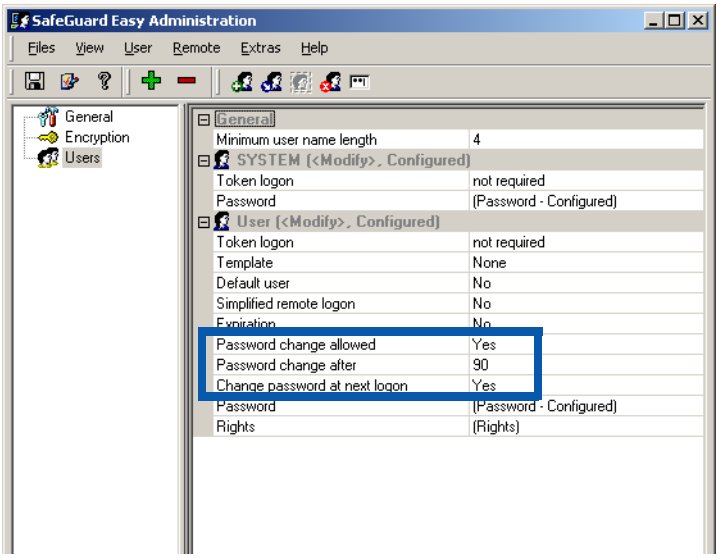
If a list of forbidden passwords already exists, you can import it. In this way you can use the same list on several workstations. The list can be created with any editor, and could look like this:



The different passwords are separated with a blank space or a line break.

> ***NOTE:***
> Users should not have access to this file!

13.6 User-specific password rules



The user-specific password rules involve options for changing the password.

13.6.1 Password change allowed

This option defines whether a user can change their SafeGuard Easy password within PBA or in Administration, or not.

13.6.2 Password change after

A SafeGuard Easy password is valid for an unlimited time period. However, there is a great danger that it will become known. To minimize the security risk, you can specify that a user must change their password after a pre-defined number of days.

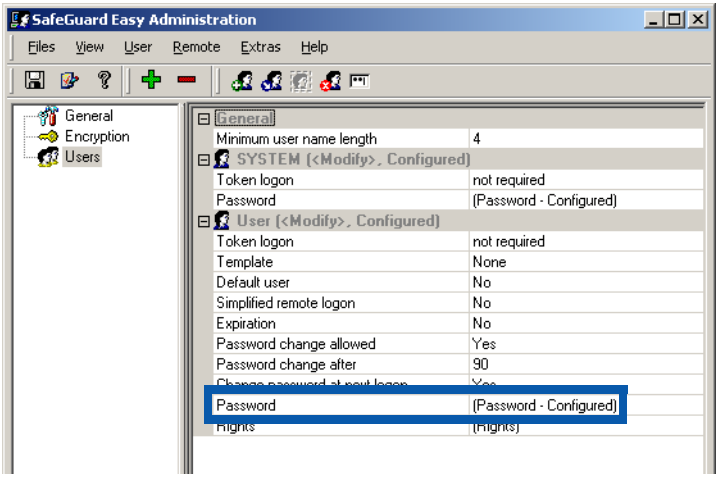
Use the direction keys to set the time period after which the user must change their password, or type it in.

The time period for the validity of the passwords can lie between 1 and 365 days. The default setting is 90 days. Once the time period has expired, the user must change their password next time they log on.

13.6.3 Change password at next logon

Specifies that the user must change their SafeGuard Easy password at their next logon. To use this function Pre-Boot Authentication must be active.

13.7 Defining a password



The choice of user passwords should be made carefully so they cannot be easily guessed. They can contain any letters (capitals or lower case), numbers and special characters (!„§$%&/()*+;,:._-), provided the combination has not been restricted by the General Password Rules.

The numbers in the number block must not be used.

If you double-click "Password", you see the dialog in which you define the password.

Specify User Password
User Password
Please type in the new password for the specified user. To prevent miss-typing you have to type the password twice.
User specified: User
Password
Confirm Password
OK
Cancel

In the top line, enter the required password and repeat it in the Confirm field below. You have to repeat the entry to prevent typing errors. The system checks that the characters entered are identical, and displays an error message if the passwords do not match up or are trivial (such as "12345" or "AAABBB"). For security reasons the entry is only represented by "*" characters. To correct entries, use the Backspace key.

You are not permitted to "copy and paste" a password: you must type it in by hand.

14 Twinboot/Boot Manager

Twinboot is a new installation variant with which you clearly separate the business and private areas of a PC.

14.1 Functionality

To protect sensitive data on a PC with Twinboot, two primary partitions must be present, with a bootable operating system on each one. Twinboot encrypts one partition (business partition), while the other one is left in plain text (private partition). The encrypted part is only accessible with the SafeGuard Easy password. The private part is not protected by SafeGuard Easy: its data is left unencrypted. The business and private partition are invisible to each other. No sensitive data can be transferred from the encrypted business partition to the unprotected private partition. If you need to exchange data between the encrypted and unencrypted partition, you can enable this via an option in the SafeGuard Easy settings.

SafeGuard Easy Boot Manager lets you choose which partition is booted (Private or Business). A menu appears on the screen and displays the different operating systems. The encrypted partition requires authentication with the SafeGuard Easy password in Pre-Boot Authentication (PBA), while the unencrypted partition requires no authentication. For this reason the Boot Manager appears and you must decide which operating system is used for booting before (possible) Pre-Boot Authentication.

The Twinboot installation requires you to activate floppy disk and removable media encryption (ZIP, MO drives). Floppy disks and removable media remain enciphered as soon as you start the PC from encrypted (business) partition. If you select the plain text (Private) partition, floppy and removable media drives are unencrypted, but SafeGuard Easy users with the appropriate user rights can temporarily switch them on or off.

> ***NOTE:***
> You can also choose to leave additional partitions encrypted or unencrypted, to suit you.

14.2 Prerequisites

- Twinboot can only be installed if only **one single hard disk** is connected. If the system recognizes two hard disks, the Twinboot option will be grayed out. You can install additional hard disks after setting up Twinboot, but no SafeGuard Easy encryption support will be provided for these additional hard disks.
- At least **two primary partitions**, with a bootable operating system on each one, must be present on the existing hard disk.
- BEFORE installing SafeGuard Easy, ensure you have partitioned the hard disk and installed all operating systems (**only Windows is supported!**). We recommend that you do not attempt to make changes later.

14.3 Example

Initial configuration

C:\	D:\	E:\	F:\	G:\
primary partition	primary partition	logical drive in extended partition	logical drive in extended partition	logical drive in extended partition
encrypted	not encrypted	encrypted	not encrypted	not encrypted
Boot drive 1	Boot drive 2			

Boot from encrypted Boot drive 1

C:\	D:\	E:\	F:\	
primary partition	logical drive in extended partition	logical drive in extended partition	logical drive in extended partition	
encrypted	encrypted	not encrypted	not encrypted	not encrypted
Boot drive 1				Boot drive 2
readable	readable	*not readable*	*not readable*	*invisible*

Boot from unencrypted Boot drive 2

C:\	D:\	E:\	F:\	
primary partition	logical drive in extended partition	logical drive in extended partition	logical drive in extended partition	
not encrypted	encrypted	not encrypted	not encrypted	encrypted
Boot drive 2				Boot drive 1
readable	*not readable*	readable	readable	*invisible*

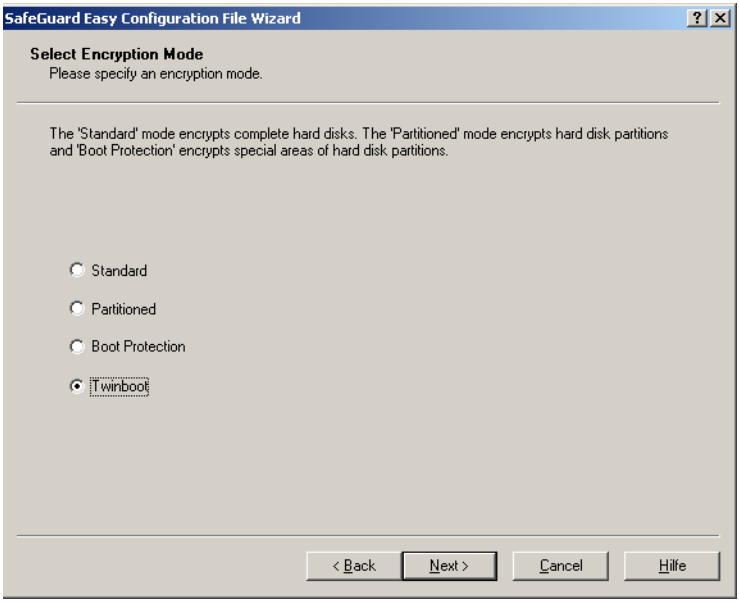
14.4 Configuring Twinboot

1. Set up two primary partitions on the computer's master hard disk and install a bootable operating system on each partition.

2. Then boot from the "business partition".

3. Start local installation of SafeGuard Easy. Confirm all the entries you see next by clicking [Next].

4. In the "Select Encryption Mode" dialog, select "Twinboot".


SafeGuard Easy Configuration File Wizard
Select Encryption Mode
Please specify an encryption mode.
The 'Standard' mode encrypts complete hard disks. The 'Partitioned' mode encrypts hard disk partitions and 'Boot Protection' encrypts special areas of hard disk partitions.
Standard
Partitioned
Boot Protection
Twinboot
< Back
Next >
Cancel
Hilfe

5. In SafeGuard Easy's administration program, select the **Encryption** folder. In addition to the Windows boot partition (=primary partition which contains the files required to booting, such as Ntldr, Boot.ini, Ntdetect.com), which is already marked as encrypted, the following disk drives must also be encrypted:

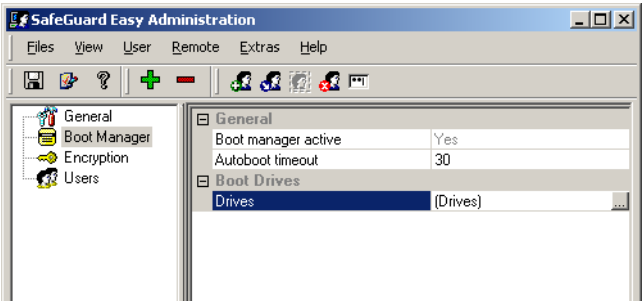
   - the Windows System drive. This contains the Windows system files (may be the same as the boot partition).
   - the drive containing the SafeGuard Easy installation folder. This ensures access to the SafeGuard Easy files.
   - A Twinboot installation also requires that floppy and removable media drives are encrypted.

6. Twinboot mode automatically activates the SafeGuard Easy Boot Manager. Go to the "Boot Manager" folder and fine-tune your settings.

NOTE:
If you select a partition to which access is forbidden, after installation, you see a dialog that says "Do you want to format this partition?". If you click [YES], you will lose all data in that partition!

14.5 Configuring Boot Manager

To configure the Boot Manager, open the Boot Manager folder in the Administration program. However, you can only see the configuration screen if you have selected encryption mode "Twinboot".



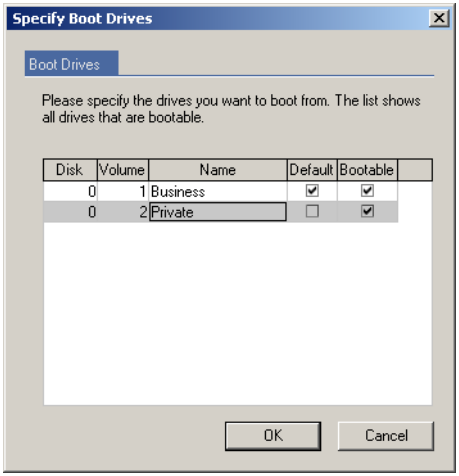
14.5.1 General settings

- **Boot manager active:**
  specifies whether the Boot Manager is switched on or off. In the case of a Twinboot installation it is switched on by default.

- **Autoboot time-out**
  The boot drive that is set as the "default" (defined in "Boot Drives") is automatically booted when the system is switched on, if the user does not select another boot drive within a set time period. You specify this time-span in the "Autoboot time-out" field. If there is no default drive, the operating system boots from the first primary partition.

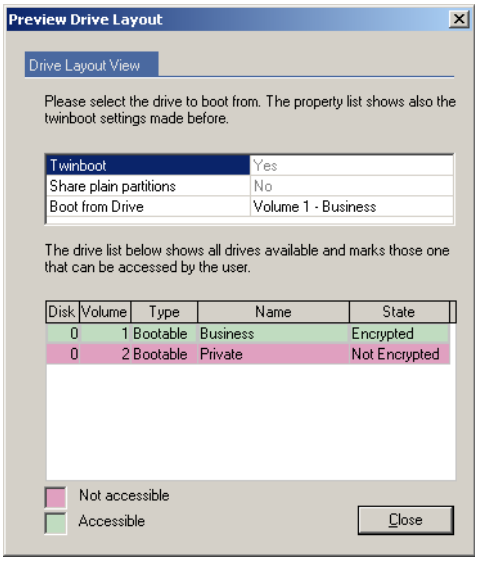
14.5.2 Boot drives

In the "Specify Boot Drives" dialog, which you open by double-clicking on "Drives", you define the properties of the Boot Manager menu.



You see a list of all **primary partitions** on the computer. We recommend you enter **meaningful** boot names to distinguish between the different bootable disk drives in the Boot Manager menu (maximum length, 40 characters. Example: "Private"). The names you enter are later displayed in the Boot Manager selection menu. Before a disk drive can be displayed in SafeGuard Easy Boot Manager, it must first be marked as "**Bootable**". You must also choose one of the displayed disk drives as the **Default drive**, which is automatically accessed during a system start if the user does not select a boot drive in Boot Manager.

You can click **Preview Drive Layout** to display the encryption status and access for each selected boot partition separately.



Twinboot:
Shows whether this encryption mode is active.

Share plain partitions (setting at Encryption tab/Twinboot/Share plain partitions):
Shows whether it is possible to exchange data between encrypted and unencrypted partitions.

Boot from Drive:
Shows the access rights dependent on the boot drive, but has NO effect on the settings made in "Specify Boot Drives".

NOTES:

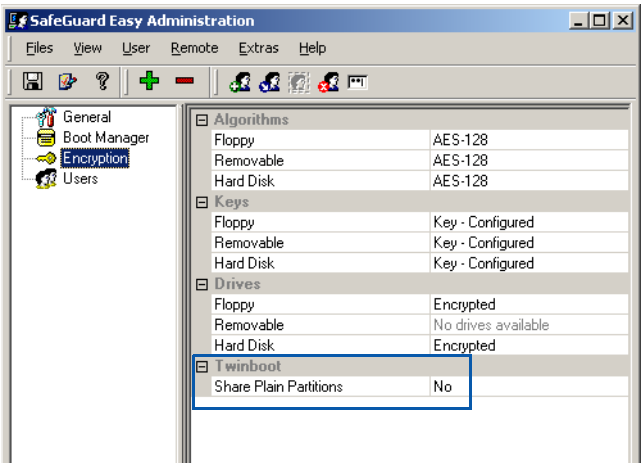
- For technical reasons the Boot Manager does not operate until the encryption/decryption processes are complete. The first restart after the encryption/decryption automatically calls the operating system on the Windows system drive without starting the Boot Manager. This often happens in Twinboot installations after the wizard is used to generate a kernel backup for the emergency floppy disk.

- The Boot Manager changes the partition type entry in the partition table to "Hidden (48h)" for each bootable primary partition that was not booted. These changes are retained in the partition table even if the FDISK /MBR command is used to delete the SafeGuard Easy MBR boot code.

  However: be careful when using FDISK /MBR! To "restore" the partition type you must uninstall SafeGuard Easy!

14.6 Exchanging data between boot partitions (Share Plain Partitions)

If it is necessary to exchange data between the business and private partitions, you can enable this in the "**Share Plain Partitions**" setting in the encryption settings.

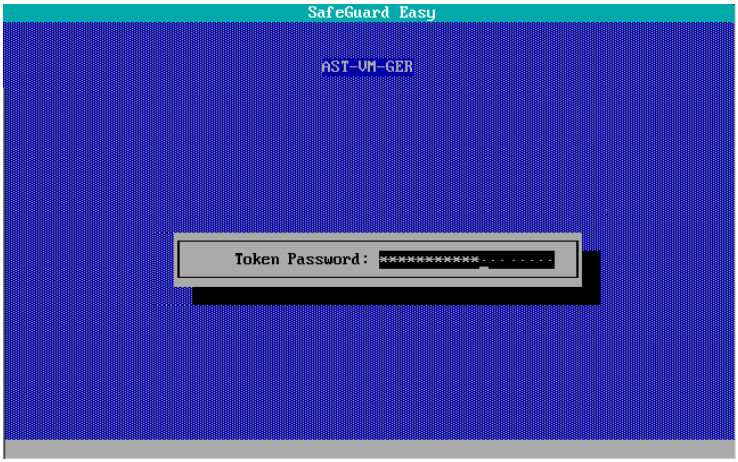


If this setting is set to "Yes" the unencrypted partitions can be accessed even if the encrypted partition has been booted.

15 Token support

Nowadays, authentication with a user name and password is not enough to meet customer needs for optimum protection against attacks by outsiders. For this reason, SafeGuard Easy offers logon with a USB token as an alternative to the "traditional" logon method, and to increase security. Token-based logon uses the principle of two-factor authentication: a user has a token (property), but can only use the token if they know the specific token password (knowledge).

To use the Aladdin eToken Pro that has been issued to them, a user simply plugs it into a USB port on their workstation, switches on the PC and waits until it stops at the Pre-Boot Authentication prompt. They then enter the Token Password at the prompt.



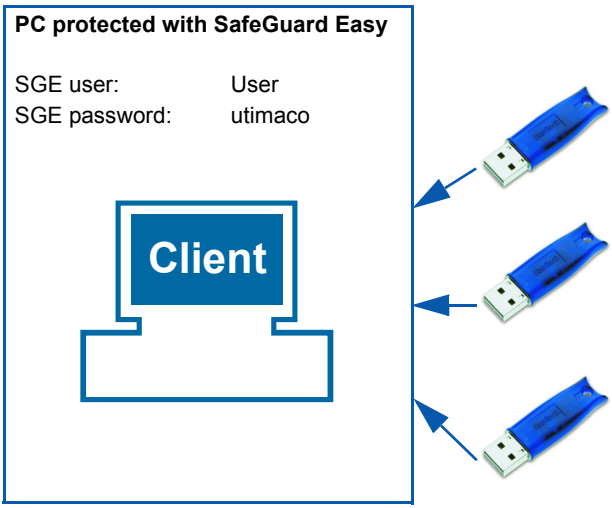
If they enter it correctly, SafeGuard Easy reads the user data from the token, passes it to PBA and then carries out the logon procedure.

If a user loses their token, the administrator can use the Challenge/ Response procedure to temporarily allow the user to log on.

15.1 Benefits of logging on using a token

- Users only have to remember the token password. When the appropriate configuration has been set up, the token or Secure Automatic Logon (SAL) takes care of logging on to SafeGuard Easy and the operating system.
- A hierarchical, centralized administration concept can be implemented in a company, for example for the creation of configuration files.
- The SafeGuard Easy user concept remains hidden from the "regular" user if this user does not know their SafeGuard Easy user data.
- If the user does not know their SafeGuard Easy user data, the mismatch between the SafeGuard Easy and Windows user can be resolved and the number of SafeGuard Easy users per workstation can be increased to any required quantity.

  If you select this option, you can implement a **roles-based access concept** and bypass the maximum number of SafeGuard Easy users permitted per workstation (15 users): in an environment where roles are used, users only know their token password, not their SafeGuard Easy access data (=SafeGuard Easy role). If the administrator issues a large number of tokens that contain the same SafeGuard Easy role, any number of token owners can share one workstation that is protected with SafeGuard Easy. Each user has different Windows access data, which ensures that they also have an individual desktop.


PC protected with SafeGuard Easy
SGE user: User
SGE password: utimaco
Client
Token 1
SGE user: User
SGE password: utimaco
Token password: 1234
Token 2
SGE user: User
SGE password: utimaco
Token password: FF06D
Token N
SGE user: User
SGE password: utimaco
Token password: a126

15.2 Supported tokens

SafeGuard Easy supports Aladdin eToken Pro, VeriSign USB Token and RSA SecurID Token.

Aladdin eToken Pro

Aladdin Pro 16K
Aladdin Pro 32K
Aladdin Pro 64K/OTP*

*SafeGuard Easy supports the Kryptochip, but not the token's One Time Password function (OTP).

Aladdin eToken NG-FLASH and NG-OTP

The default password for a (blank) Aladdin eToken is "1234567890".

VeriSign USB token

OEM version of the Aladdin eToken.

The serial number printed on the USB must start with "ALPR".

RSA SecurID 800-Token

SafeGuard Easy supports the Kryptochip, but not the token's One Time Password function (OTP).

WARNING: A specific version of RSA Authenticator Client is required. For more information, please contact your token manufacturer. The RSA Authenticator Utility is no longer supported by SafeGuard Easy Version 4.50.

The default password for the RSA SecurID 800 Token is "PIN_CODE".

15.3 Token functions

Action	Aladdin eToken/ VeriSign USB Token	RSA SecurID 800 Token	Lenovo fingerprint reader
Log on in pre-boot authentication	X	X	X
Log onto SafeGuard Easy Administration	X[1]	X[2]	--
Log onto configuration files	X[1]	X[2]	--
Log onto Windows	X[1]	X[2]	X[3]
Lock Windows workstation	X[1]	X[2]	--
Faster SafeGuard Easy user changeover	X[1]	X[2]	--

[1] Only with "Aladdin Runtime Environment" (PKCS#11 module)

[2] Only with "RSA Authenticator Client" (PKCS#11 module)

WARNING: To perform tasks at operating system level you require a specific version of the RSA Authenticator Client. For more information, please contact your token manufacturer. The RSA Authenticator Utility is no longer supported by SafeGuard Easy Version 4.50.

[3] Only with Lenovo ThinkVantage fingerprint software

15.4 Install token support

How to install the Token support:

1. Start SafeGuard Easy setup.

2. Select installation options and encryption mode.

3. In the configuration settings, select **General/Authentication/Logon**. Here you define how a user is to log on to Pre-Boot Authentication with a keyboard, token or fingerprint:

Keyboard	Users use the SafeGuard Easy access data to log on in PBA.
Aladdin eToken	Users use the token password for the Aladdin eToken to log in PBA.
Fingerprint	Users use their fingerprint to log on in PBA.
RSA SID 800	Users log on using the token password for the RSA SID token.
RSA SID 800 Random	Users log on using the token password for the RSA SID token. "Random" means that a random password generated by SafeGuard Easy will be written to the token. Users do not know this password.

4. If you have selected a token (Aladdin, RSA) or fingerprint, select the **Login mode**.

with token only	This option means that SafeGuard Easy requires token-based logon for all SafeGuard Easy users on a workstation. WARNING: If the "with token only" method is selected, a user can only log on in PBA if the token already contains valid SafeGuard Easy data. If the token is blank you cannot log on in PBA.
token optional	This option means that only particular SafeGuard Easy users on a workstation can log on with a token or manually with SafeGuard Easy user data. With this option one single SafeGuard Easy user can be forced to use a token while all other SafeGuard Easy users can select token or SafeGuard Easy user data to log on.

5. If you have selected "Token optional" then select **User/<username> / Logon** and then specify who must log on with a token.

   You can for example specify that a particular user called "user_1" must log on with a token (setting "Required"), but that another user called user_SYSTEM can choose between using a token and entering their SafeGuard Easy access data manually (setting "Not required").

6. Select **General/Authentication/Issuing mode** to define who is permitted to write SafeGuard Easy access data to a token.

SafeGuard Easy offers several issuing modes:

User	Allows user to issue a “blank” token in the PBA. In this context, “Blank” means that the token does not contain any SafeGuard Easy data.
External Commitment	Forces user to call helpdesk. Helpdesk allows the user to issue the token in the PBA by using the Challenge/Response procedure.
Central	User receives an issued token and is never allowed to issue the token in the PBA.

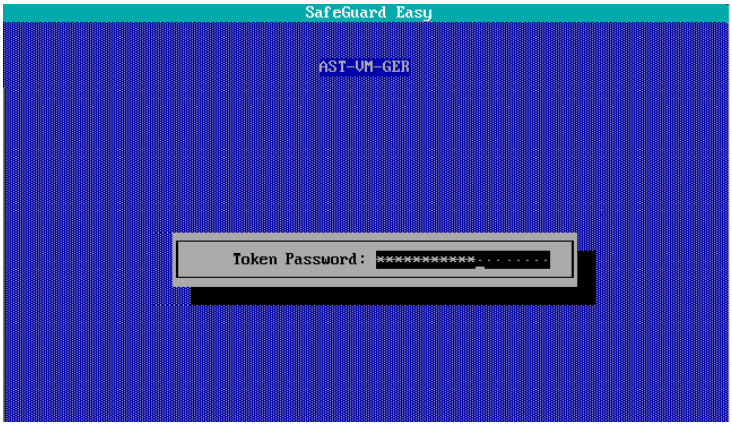
7. Close the installation procedure. You have made all the settings involved in token-based logon.
8. Restart the PC.

15.5 Logging on for the first time with a token in the pre-boot authentication

To log on using a formatted, "empty" token:

1. Insert the token in the USB Port.
2. Switch on the PC and wait until it stops at pre-boot authentication.
3. Enter the token password

   The default for Aladdin eToken is 1234567890.
   The default for RSA 800 Token is PIN_CODE

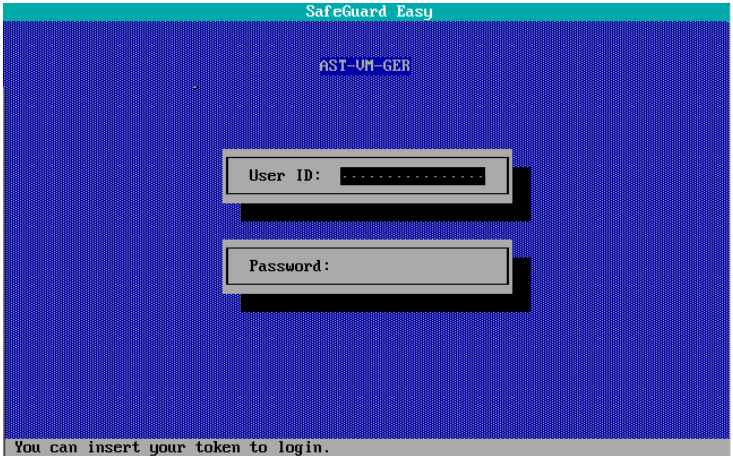


4. Remember that the token's default password may be a security risk and you should change it (you can use a maximum of 32 characters here).

   Enter your new token password.

5. Enter the SafeGuard Easy access data (user name and password). The data is written to the token.

   The pre-defined setting mode specifies whether a SafeGuard Easy user is permitted to write access data to the token!



6. The procedure for logging on to SafeGuard Easy continues. The next time you log on you will only need the token password.

15.6 How to change the token password

To change your password in the Pre-boot authentication phase:

1. Insert the token in the USB port.
2. Start the PC.
3. Enter the token password in the pre-boot authentication phase.
4. Press [F10].
5. Enter your new token password.

The following rules apply to new token passwords:

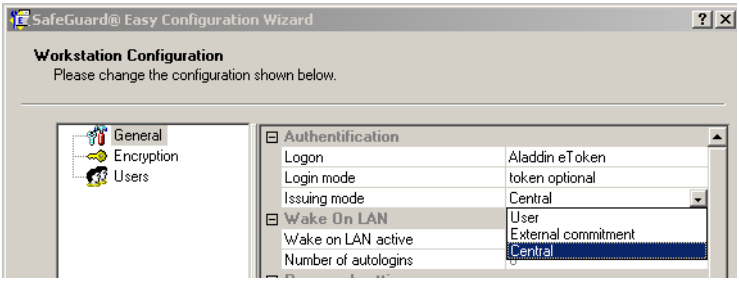
- the new token password may not be the same as the old one.
- the new token password must not be easy to guess (e.g. "1234" or "asdf")

15.7 How to change or delete SafeGuard Easy access data

You can delete or change SafeGuard Easy access data via token Administration (see also 'Issuing a token with the Token Administration').

15.8 Issuing a token

When a token is "issued", data is written to the token, and then used for authentication.



"Issuing Mode" specifies who can write SafeGuard Easy access data to the token.

The user who issues the token must know the token password. Otherwise, it is impossible for any instance to issue the token.

15.8.1 Token issuing mode

Issuing mode "User"
The user is permitted to enter their own SafeGuard Easy access data, after PBA is processed for the first time. This data is then written to the token. Naturally, it is a prerequisite that the user knows the access data for a SafeGuard Easy user profile that is registered on the workstation.

Issuing mode "External commitment"
The user can only write SafeGuard Easy access data to the token ("issue" data to it) after exchanging a challenge and response code.

If the token contains no suitable SafeGuard Easy data, the user is prompted to request a challenge code by pressing function key [F9] in PBA, and then to contact the Helpdesk/Support. The support member starts the Response Code Wizard, completes the authentication dialog and enters the challenge code. As "Remote Command" the administrator selects "Grant permission to issue token". The administrator passes the generated response code to the user via e-mail, SMS or telephone. The user enters the response code in the fields intended for that purpose and is afterwards able to issue the token.

This approach involves a central unit in a company (such as the Helpdesk/Support department), and in some circumstances it requires more time and effort. On the other hand, it prevents more than one token being issued for one machine without the central Support department being informed.

Issuing mode "Central"
The user receives a token issued by a central helpdesk/support and can log on. "Token Administration" is responsible for issuing the token centrally. You will find an overview of issuing a token with the Token Administration in 'Issuing a token with the Token Administration'.

15.8.2 Unattended issuing

Tokens can be issued using an automated method. To do so, a Visual Basic script (vbs) is required. After this vbs file is executed, all the defined information (logon data for Windows, SafeGuard Easy, Terminal Server, SSO etc.) is written to the token at once. We recommend you use this method for issuing a very large number of tokens for the first time.

Example of a vbs script

Below you find an example visual basic script. Open an editor, copy the example line by line, and save it as a vbs file. Afterwards, fill in the required logon information. For example, replace *User PIN* with the token's User PIN.

```
dim scard
dim res
dim slotID
dim pin
dim mustChangePIN
dim userID
dim password
dim domain
dim terminalServer
dim fileName
dim cerFile
dim linkFile
dim pkcsFile
dim protFile
dim cardInserted
dim authFile
dim configFile

set scard = WScript.CreateObject("SCardAdmScriptAPI.SCScriptAPI")

' *** Card Initializing Important !!!! ***
slotID = 0
res = scard.Initialize(slotID)

' *** Card Inserted? ***
cardInserted = scard.IsCardInserted()
if cardInserted then
WScript.Echo("Card is inserted")
else
WScript.Echo("NO Card in Slot")
```

```
end if

' *** Reading Serial number ***
serialNumber = scard.GetCardSerialNumber()
WScript.Echo(serialNumber)

' *** Change User PIN ***
pin="New User PIN"
oldPIN="Old User PIN"
res = scard.SetUserPIN(oldPIN,pin)

' *** Change Security Officer PIN ***
pin="New Security Officer-PIN"
oldPIN="Old Security Officer-PIN"
res = scard.SetSOPIN(oldPIN,pin)

' *** Initializing User PIN ***
pin="New User PIN"
soPIN="Security Officer-PIN"
res = scard.InitUserPIN(soPIN,pin)

' *** Logon ***
pin = "User PIN"
res = scard.LoginUser(pin)

' *** Force User PIN change!  1=Force Change   0=Don't change PIN ***
mustChangePIN = 0, 1
res = scard.SetUserChangePIN(mustChangePIN)

' *** Windows Account Data ***
userID = "Windows user name"
password = "Windows user password"
domain = "Domain"
res = scard.SetWindowsAccount(userID,password,domain)

' *** Set Sgeasy account data ***
configFile = "<absolute path and SGE Install configuration file name>"
user ID = "<the SGE user whose data is to be written to the token>"
authFile = "<absolute path of the file that contains the authentication data for the
            configuration file >
res = scard.SetSGEasyAccount4 (configFile,userID,authFile)
WScript.Echo(res)

' *** Show Windows User ID ***
userID = scard.GetWindowsAccount()
WScript.Echo(userID)

' *** Add MultiDesktop Role(s) ***
userID = "Role name"
```

```
password = "Role name's password"
domain = "Domain"
res = scard.AddMultidesktopRole(userID,password,domain)

' *** Add Terminal Server Account(s) ***
userID = "TS user name"
password = "TS-Password"
domain = "Domain name"
terminalServer = "Name of the TS"
res = scard.AddTerminalServerAccount(userID,password,domain,terminalServer)

' *** Create Certificates ***
' 1) SSCertImport
fileName = "PKCS#12 File"
password = "Password for PKCS#12 file"
res=scard.ImportCertificate(fileName,password)

' 2) SSCert by SC
userID = "Windows user name"
cerFile = "CER file's name"
linkFile = "CSV file's name"
res=scard.CreateSSCertSC(userID,cerFile,linkFile)

' '3) SSCertBySW

userID = "User name"
cerFile = "Path and name of the Certificate file (CER file)"
linkFile = "Path and name of the Link file (*.csv)"
pkcsFile = "Path and name of the PKCS#12 file"
protFile = "Path and name of the Log file"
res=scard.CreateSSCertSW(userID, cerFile, linkFile, pkcsFile, protFile)

' *** Logoff Important !! ***
res = scard.Uninitialize()
```

General Notes

- Do not remove the quotation marks! A line within the script may look like this: password=”Sales”.
  If no entry is required, leave the quotation marks empty (e.g. password = ““).
- Always enter the correct token PINs. Otherwise the system stops and displays an error report.
- After you executed a script, an existing Windows Account will be replaced.
- After executing a script a new MultiDesktop role is created. Any existing roles will not be replaced or removed.
- An existing Terminal Server Account on the token will not be removed or replaced after a script is executed.

Description of “Set SafeGuard Easy account data” in the script

- **configFile**
  Specifies the absolute path and name of the SafeGuard Easy configuration file.

  For example: configFile = “D:\Install.cfg“

  The configuration file must have been created using the SafeGuard Easy Configuration File Wizard before it can be activated automatically. It must be a configuration file that has the "Install" property.

  It is essential that the configuration file contains these SafeGuard Easy user profiles:

  1) The user whose data is to be written to the token under *UserID* (e.g. "USER")
  2) The user who is to log onto the configuration file under *authFile* (e.g. "Helpdesk")

- **userID**
  The SafeGuard Easy user whose data is to be written to the token. This user's data must be present in the configuration file.

  For example: userID = "User"

- **authFile**
  Absolute path of the file that contains the SafeGuard Easy profile data used to log on to the configuration file.

  For example: authFile = "D:\Token.PWD"

  The encrypted Token.PWD file contains the SafeGuard Easy profile data. Token.PWD is generated by the SGECPWF.exe tool. (this is stored on the SafeGuard Easy CD in the \Tools directory).

Executing a script
How to execute a vbs script:

1. Install Token Support and the Token Administration system.

2. Write/Copy the complete script line by line into an editor and save the file (e.g. token.vbs)

3. Fill in the required information.

4. Connect a token to the PC.

5. Run the script, for example by double-clicking it in the Windows Explorer.

6. The system issues the token.

15.9 Token support for SafeGuard Easy Administration Tools

SafeGuard Easy provides different tools (Administration, Configuration File Wizard, Response Code Wizard) for administrative tasks. Some actions within these administration tools require SafeGuard Easy data, e.g. when logging on to Administration or during authentication to a base configuration file in the Configuration File Wizard.

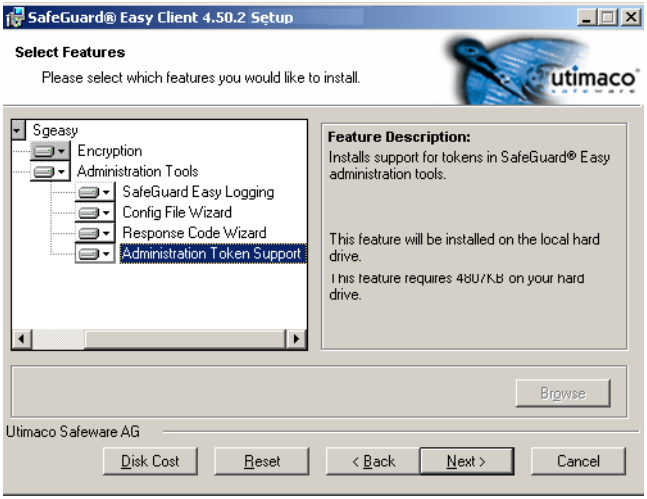
Token support in SafeGuard Easy works in a similar way to logon during PBA: after the token has been inserted, the user is prompted to enter the PIN. When they do so, the system reads the SafeGuard Easy password and user name from the token and logon (authentication) is performed.

Token-based logon to the administration tools is optional and also applies for when SafeGuard Easy is to be uninstalled.

15.9.1 Enabling logging on to the Administration Tools with a token

The procedure for activating token support for administrative tools is as follows:

1. During installation the "Administration Token Support" installation option must be activated on a workstation.



2. Restart the workstation.
3. Install these software packages:

Token used	Necessary software
Aladdin e Token VeriSign USB token	Aladdin e Token Runtime Environment (see also http://www.utimaco.com/etoken)
RSA SecurID 800	RSA Authenticator Client

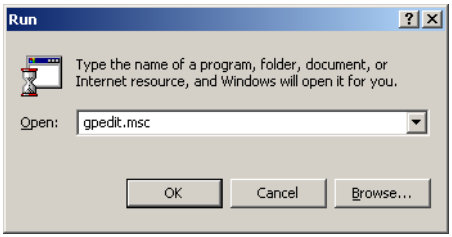
4. Register the token's PKCS#11 module.

15.9.2 Registering the token's PKCS#11 module

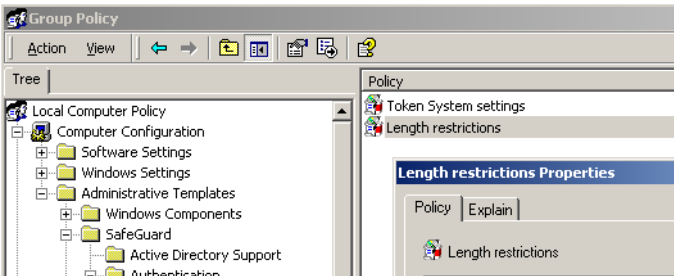
To "tell" SafeGuard Easy about a token, you must register the token's PKCS#11 module.

1. Click the [Start] button in the Windows task bar and select the *Run* command.

2. In the Open: field, type the command `gpedit.msc`.

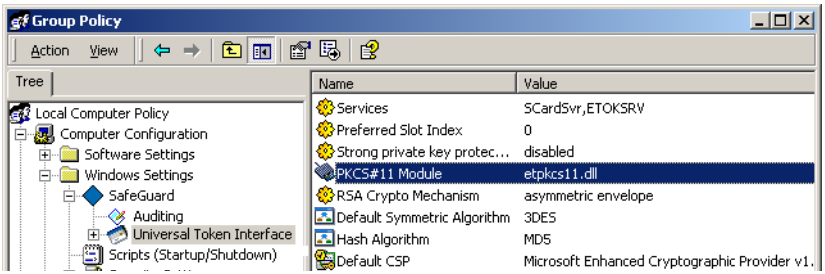


The Microsoft Management Console appears in



3. Under

   Computer Configuration
   \Windows Settings
   \SafeGuard
   \Universal Token Interface
   enter the following settings:



Token used	Necessary settings
Aladdin e Token VeriSign USB token	Services: SCardSvr, ETOKSRV PKCS#11 module: "etpkcs11.dll" (from SYSTEM32 folder)
RSA SecurID 800	Services: SCardSvr PKCS#11 module: "pkcs11.dll" To add the PKCS#11 module for RSA ensure to enter the full path name. WARNING: A specific version of RSA Authenticator Client is required. For more information, please contact your token manufacturer. The RSA Authenticator Utility is no longer supported by SafeGuard Easy Version 4.50.

4. Save the settings.
   You can now use a token to log on to SafeGuard Easy's Administration Tools.

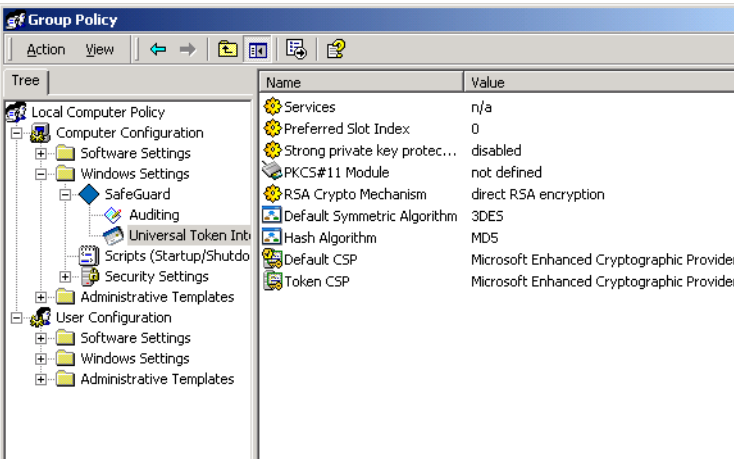
15.9.3 Universal Token Interface

The Universal Token Interface is an API which is used by Utimaco applications to communicate with different tokens. It provides functions for accessing (read/write) private data stored on a token, and it can be used to encrypt/decrypt, sign and verify data by using the RSA key pair stored on the token.

The Universal Token Interface node is displayed only if Administration Token Support is installed.

The settings for the Universal Token Interface are stored in the MMC at:

Computer Configuration
\Windows Settings
\SafeGuard
\Universal Token Interface



The following settings can be configured:

Services
Here you need to specify the services that are necessary for using the token, and therefore have to be started, before the Universal Token Interface is initialized.

`SCardSvr`
Operating system's smartcard service. This entry is mandatory.

Some tokens also require additional token-specific services, which you must also specify. Separate each service with a comma.

Preferred Slot Index
A token requires a specific slot index. Enter the slot for your token here. If the PKCS#11 module for the SafeGuard Smartcard Provider is selected, slot 0 is entered here automatically.

> ***NOTE:***
> Ensure your token is connected to the specified slot.

PKCS#11 module
The PKCS#11 module is responsible for communication (read/write) with the token.

Enter the appropriate PKCS#11 module for your token here.

PKCS#11 module, services, slots

Token Provider	Software	PKCS#11 module	Services
Aladdin (USB Token)	most recent Aladdin Runtime Environment (RTE)	eTpkcs11.dll	SCardSvr, ETOKSRV
Verisign (USB token)	see Aladdin	see Aladdin	see Aladdin
RSA SecurID Token	most recent RSA Authenticator Client	pkcs11.dll	SCardSvr

Strong Private Key Protection
If enabled, the user will be prompted for authentication every time the private key is used in an application.

Default CSP
All CSPs available on you system are displayed here. You can choose which one to use for operations with the public key.

We recommend you use the Microsoft Enhanced Cryptographic Service Provider.

Token CSP
Specify the CSP for the token you are using. If you use Utimaco smartcards, select the Utimaco Universal Smartcard CSP.

RSA Crypto Mechanism
For CSPs which do not offer direct RSA encryption, the **asymmetric envelope** option is provided. If you use it, bulk data is encrypted using a selectable symmetric algorithm. RSA encryption is applied to the key used.

Default Symmetric Algorithm
Choose the algorithm for symmetric encryption of bulk data, if you have selected **asymmetric envelope** as the RSA Crypto Mechanism.

Hash Algorithm
Select the hash algorithm to be used.

15.10 Logging on to the operating system with token

If the logon to SafeGuard Easy was successful, the operating system then prompts requires the user to enter valid access data. This means that, during token-based logon, the user is prompted to enter data twice: once in the Pre-Boot phase (token password) and then at the normal operating system logon.

NOTES:

- The SafeGuard component used to log on to the operating system supports passwords with a maximum length of 63 characters.

  We recommend that you do not exceeded the maximum limit for the token password.

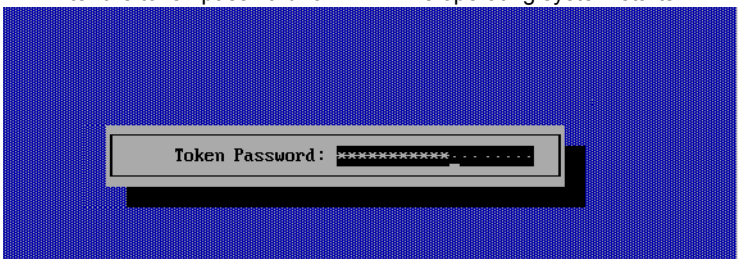
- It is a prerequisite that particular drivers (PKCS#11, Cryptographic Service Provider (CSP)) are made available to support the token at operating-system level.

15.10.1 Issuing a token with operating system data

How to issue a token with operating system data:

1. Insert the (formatted) token in the USB port and switch on the PC.

2. Enter the token password for PBA. The operating system starts.



3. Enter the token password and click [OK].

4. Since the token does not yet contain Windows logon data, you are prompted to confirm that the token should be issued.

5. The system displays the *Issue Token with Windows data* dialog. Enter your Windows user name and password and click [OK].

A dialog confirms that the token has been successfully issued. After the next reboot you are automatically logged on to the operating system.

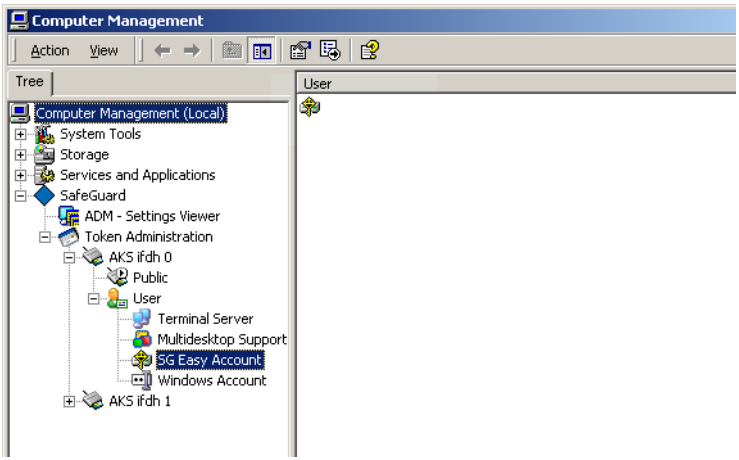
15.10.2 Saving Windows data in the SAL file

The operating system data is synchronized with the encrypted SAL file, `SGSAL.dat`, after every successful login using a token, provided that **the SafeGuard Easy "Token optional" logon procedure** was selected. This guarantees that the user can access the data, especially in emergencies (user loses token with Windows data, or similar). If the user changes their Windows data, the `SGSAL.dat` is also updated.

15.11 Issuing a token with the Token Administration

If the Token Administration is installed, you can write the following data to the token:

- Token Password (PIN)
- Data for SafeGuard Products
- Windows logon data



Multi-desktop support and Terminal Server only work when combined with SafeGuard Advanced Security.

15.11.1 Installing the Token Administration

1. Install from the \TOOLS folder of the installation CD

   - TokenAdmin.msi
   - SCAdmin_SGEasy.msi

2. To secure the link between the token and SafeGuard GINA, the PKCS#11 module must be made known to the token. You will find details in 'Registering the token's PKCS#11 module'.

3. Connect the token with the PC.

4. Select Start/Settings/Control Panel/Administrative Tools/ **Computer Management**.

   In the Computer Management "SafeGuard" folder you can see "Token Administration".

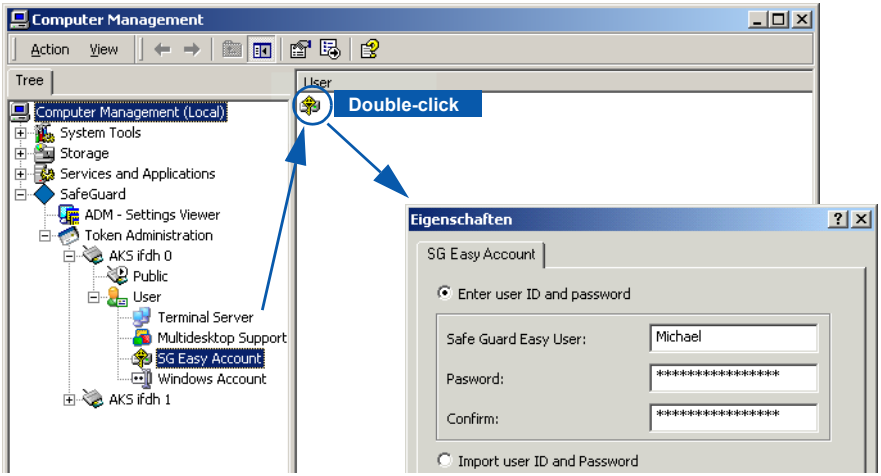
5. Log on to Token Administration with your token password.

6. Open the **User** folder.

7. Select the **SGEasy Account** folder.

8. Open the **Properties** dialog by double-clicking on the SafeGuard Easy icon in the "User" column.

9. Select "Enter user ID and password" and enter the user name and password.



10. Confirm your data with [OK].

The token now contains your data.

You will find more information on this subject in the Utimaco Knowledge Database http://www.utimaco.com/myutimaco.

Use the Knowledge database's "Search" field to look for key words like "Token Admin".

15.11.2 Removing SafeGuard Easy data from the token

To delete token data, select the "Delete" command in the "Sgeasy Access Data" context menu. The same is true for removing Windows access data.

15.11.3 Importing the SafeGuard Easy data from a configuration file

If you import the data, the SafeGuard Easy user data (name and password) are written to the token from an existing configuration file. This procedure is suitable if the issuer does not know the SafeGuard Easy user password or should not know it.

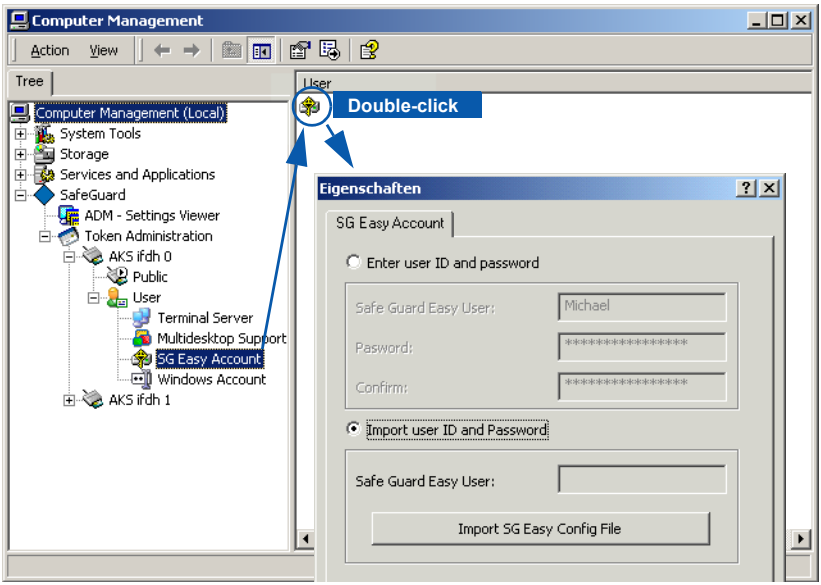
How to import SafeGuard Easy data:

1. Log on to Token Administration.

2. Open the **User** folder.

3. Select the **SGEasy Account** folder.

4. Open the **Properties** dialog by double-clicking on the SafeGuard Easy icon in the "User" column.

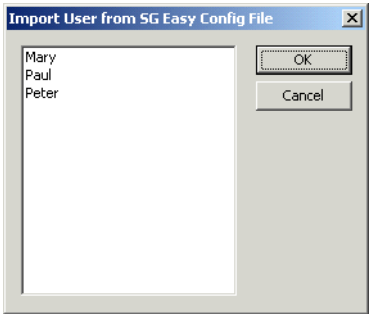


5. Select “Import user ID and Password”.

6. Click the [Import SG Easy Config File] button and select the configuration file

7. Log on to the configuration file with SafeGuard Easy credentials that are available in the file.

8. A new dialog is displayed, listing all users entered in the selected configuration file. Select the relevant SafeGuard Easy user.



9. Confirm your selection by pressing [OK]. The data is then written to the token.

15.12 Quickly changing the SafeGuard Easy user

In most cases, all SafeGuard Easy users who share a PC have the same rights. However, it sometimes happens that several users with different SafeGuard Easy authorization profiles need to use the same PC. Normally, (without token-based logon) a SafeGuard Easy user can only be changed if the PC is shut down completely and the new user then logs on during PBA with their own profile data. In some situations this might take quite a while. Users are happiest if they lose as little time as possible between the logging off as the old user and the desktop appearing for the new user.

If a token is used, the time-consuming process of shutting down and restarting the PC for a SafeGuard Easy user changeover is not necessary. In this case, simply logging off from Windows is enough. In the Windows logon dialog the token owner inserts their token in the USB port and authenticates themselves by entering their PIN. They are then logged on with the SafeGuard Easy (and Windows) authorization profile stored on the token. However, before you can carry out a user changeover, PBA must be active and valid SafeGuard Easy data must be entered during it.

15.12.1 Prerequisites

1. Install SafeGuard Easy and activate PBA.

2. Write SafeGuard Easy.

3. To quickly change a SafeGuard Easy user, close the Windows session by selecting Start/Shut Down/"Log off <User>" or by pressing [Ctrl] + [Alt] + [Del] and then clicking on Log Off.

15.12.2 Example

How the quick change works:

1. User 1 inserts their token and switches the PC on.

2. PBA appears. User 1 enters their token PIN during PBA.

   The token contains this SafeGuard Easy profile data:
   User name: *User1*
   Password: *password1*
   SGE rights: *none*

   If Windows data has also been saved to the token the user is automatically logged on to SafeGuard Easy and Windows without having to enter any other data.

   The SafeGuard Easy profile of user 1 is active. The user has no SafeGuard Easy rights.

3. User 1 finishes their work, and logs off from Windows via Start/Shut Down/Log off "User 1" (or by pressing: [Ctrl] + [Alt] + [Del]) and then clicking on Log Off. After they have logged off they remove their token.

4. The Windows logon dialog appears.

5. User 2 inserts their token (with SafeGuard Easy and Windows data) in the USB port, enters their token PIN and is then logged on with their SafeGuard Easy profile data.

   User name: *User2*
   Password: *password2*
   SGE rights: *Toggle floppy drive encryption*

   The SafeGuard Easy profile of user 2 is active. This user has the right to switch floppy encryption on and off.

15.13 Remote help

Remote administration is always needed if the user and administrator are physically apart (for example, if the user is a sales representative) and the administrator cannot resolve an error personally, on site.

Remote administration can be necessary in the following situations:

- User loses token
- User forgets token, for example they leave it at home
- User no longer remembers token password

In all these cases the SafeGuard Easy Challenge/Response procedure helps. The Challenge/Response procedure supports the system administrator by, for example, permitting a particular number of logon attempts without the user needing their token. The use of Challenge/Response is therefore a way to give the user access to the system if their token is not available or they have forgotten their token password. Nevertheless, the procedure also ensures that only a legitimate user can log on.

15.13.1 Prerequisites for Challenge/Response

Successful token-based remote administration requires the following token settings on the SafeGuard Easy client:

- Login Mode: token optional
  (see General/Authentication/Login Mode)
- Logon: required
  (see Users/<username>/Logon)

NOTES:

- The user must know the logon data for the SafeGuard Easy user on the user PC! Otherwise it is not possible to initiate the Challenge/Response procedure (unless the administrator tells the user the access data for a SafeGuard Easy user).
- The Challenge/Response procedure cannot be used to permanently deactivate token support.

15.13.2 Challenge/Response examples

The following example show the user's and administrator's tasks if a token has been lost/forgotten or the token password is no longer available.

All examples require these settings on a SafeGuard Easy client:

- Login Mode: token optional
  (see General/Authentication/Login Mode)
- Issuing mode: user
  (see General/Authentication/Issuing Mode)
- Logon: required
  (see Users/<username>/Logon)
- Pre-Boot Authentication enabled
- Secure Auto Logon (SAL) enabled

User forgets token

User	Administrator/Support/Helpdesk
The user enters their SafeGuard Easy data, and presses [F9] to request the challenge code. The user calls the administrator/ Support/Helpdesk.	
	Checks that the caller really is the actual user. Runs the Response Code Wizard. Asks the user for the challenge code and enters it. In the "Remote command" dialog, selects the "**Logon without required token for X logons**" option. Tells the user the generated response code.
The user enters the response code in the fields intended for that purpose. They can now log on for PBA x times without a token. For logon to the operating system (user does not know the data): the SAL file is opened, the user's operating system data is selected and the logon is performed.	

User loses token

User	Administrator/Support/ Helpdesk
	Sends the user a new (empty) token with the default password.
The user enters their SafeGuard Easy data, and presses [F9] to request the challenge code. Calls the administrator/support/ helpdesk.	
	Runs the Response Code Wizard. Asks the user for the challenge code and enters it. In the "Remote command" dialog, selects the "**Grant permission to issue a token**" option. Tells the user the generated response code.
The user enters the response code in the fields intended for that purpose. They now log on. Inserts the new token next time they boot the PC, enters the token password and writes the SafeGuard Easy access data to the token (if token has not yet been issued). The user does not personally have to write the operating system data to the token: it is automatically read from the SAL file and saved to the token during logon.	

NOTE:
If the new token has already been issued via Token Administration, no Challenge/Response procedure is necessary. The administrator only needs to tell the user the token password.

User forgets token password

User	Administrator/Support/ Helpdesk
Use the Challenge/Response procedure to grant the user a one-time right to log on without using a token (see "User forgets token")	
User is logged on to SafeGuard Easy and Windows without token via Challenge/ Response procedure. Inserts the Token into the USB port.	
	Uses the Token Administration's Remote function to connect to the user's PC, changes the token password and sends it to the user via e-mail, SMS, etc. Tells the user the new token password. Prerequisites: - Administrator knows the administrator password for the token. - User PC must be on the network. Token Administration must be installed both on the administrator PC and user's PC. - Token Administration must be installed both on the administrator pc and the user PC. - token contains an Administrator Password. The administrator password is the same as the Security Officer PIN in Token Administration.
Reboots the PC and logs on with the token.	

15.13.3 Administering token remotely with the Token Administration

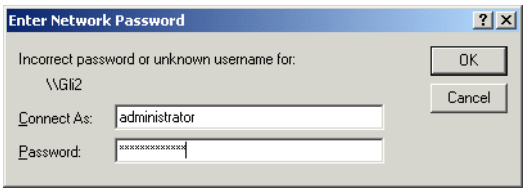
Remote Administration helps users in emergency situations, e.g. if they have forgotten their user PIN and cannot log on any more.

If a token should be administered remotely,

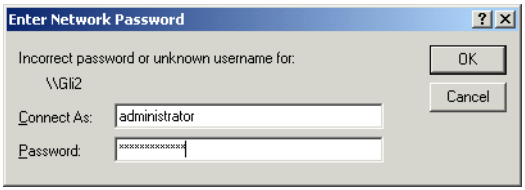
- a network connection between user and Administrator workstation has to be established.
- on the Administrator's workstation the Token Administration must be available
- on the user workstation, Token Support and Token Administration must be installed and the token must be connected.
- the user of the Administrator workstation must know the Security Officer PIN of the user's token.

How to administer a token remotely as a system administrator:

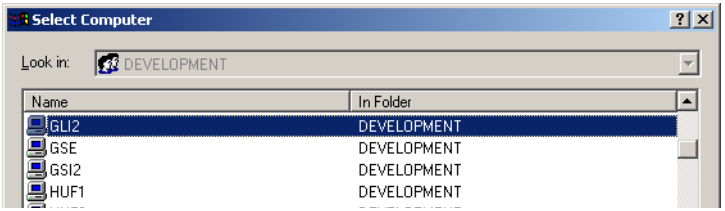
1. Establish a connection to the user workstation.



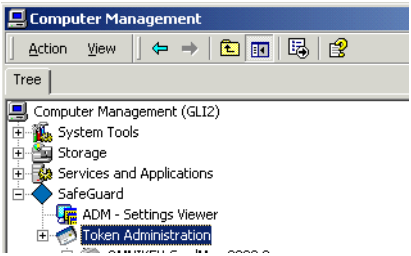
2. Establish a connection to the user workstation via the Computer Management system (“Connect to another computer...” command).



3. Select the user workstation (in this case “GLI2”).



4. Open the Token Administration on the administrator PC.



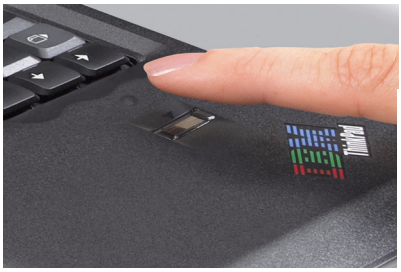
5. Log on to the Token Administration with Security Officer PIN.

The user PIN of the token connected to the user PC can now be unblocked or changed.

16 Lenovo Fingerprint Sensor

Nowadays users have to remember various combinations of numbers so that they can access their notebook or PC. Unlike a token or a password, you only need to give a fingerprint once and you cannot get it wrong (like a password) or forget it (like a token).

Fingerprint readers are already directly integrated in some Lenovo notebooks. However, you can also use a fingerprint to log on via external USB keyboards or USB readers.



SafeGuard Easy now links a user's finger with SafeGuard Easy's access data. To log on, all you need to do is swipe your finger over the reader and the SafeGuard Easy log on procedure runs automatically.

Benefits of logging on using a fingerprint

- Security: no password or token required
- Convenience: automatic logon to SafeGuard Easy and Windows (or any application that requires authentication)

Action	Lenovo Fingerprint reader
Log on in pre-boot authentication	X[3]
Log onto SafeGuard Easy Administration	--
Log onto configuration files	--
Log onto Windows	X[3]
Lock Windows workstation	--
Faster SafeGuard Easy user changeover	--

[3] Only with Lenovo ThinkVantage fingerprint software

16.1 Requirements

- Lenovo PC/Lenovo notebook Series 5x or 6x/
- We recommend you use the latest BIOS version.
- Lenovo fingerprint reader in the notebook, USB keyboard with fingerprint reader, USB fingerprint reader.
- SafeGuard Easy from version 4.30 upwards
- Supported ThinkVantage fingerprint software (Minimum):
  - ThinkVantage Fingerprint Software 5.5.0
    For versions 5.60/5.61upwards you need to change the settings in the following registry branch:
    HKEY_LOCAL_MACHINE
    SOFTWARE
    Protector Suite QL
    1.0

    Set the DWORD value "**BiosFeatures**" to "2".

16.2 Supported hardware

SafeGuard Easy supports the Lenovo PC /notebook series that has been available since Fall 2005.

Supported notebook series	Z60/Z61
	T60/T61
	X60/X61
	R60

Supported desktop series	A51
	A52
	M51
	M52
	M52e

Notebook series that are not supported	3000
	T4x

Tablet PC notebooks that are not supported	X41
	R61

NOTES:

The Lenovo 3000 notebook series is not supported because it uses a different supplier's fingerprint reader.

You must connect a keyboard to a tablet PC before you can log on using a fingerprint. During pre-boot authentication you need to type in an entry to link SafeGuard Easy access data with the fingerprint! Handwriting recognition is not possible during Pre-Boot Authentication.

16.3 Installing Lenovo fingerprint support

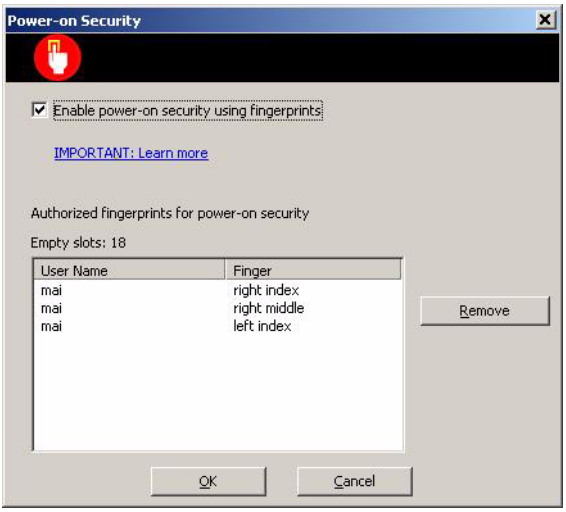
> ***WARNING:***
> If you use a fingerprint to log on, the SafeGuard Easy "standard user" function is not supported. If a SafeGuard Easy user is to be linked with a fingerprint, they must always know their user name and password for SafeGuard Easy.

This is how you install fingerprint support:

1. Install the ThinkVantage fingerprint software (if it is not already present).
2. Use this software to enroll one or more of your fingerprints. The enrolling procedure links these fingers with the Windows logon data (to find out how to enroll a finger, please refer to the ThinkVantage fingerprint software help or go to http://www-307.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-58403).
3. To test the fingerprint, reboot the PC/notebook. After it has rebooted, swipe your enrolled finger over the reader. You are now automatically logged on to Windows.

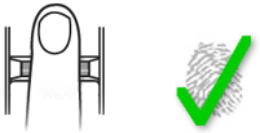
4. Start the ThinkVantage fingerprint software's Control Center.

5. In the initial screen, select Settings and then Power On Security. The "Power-on Security" dialog appears.

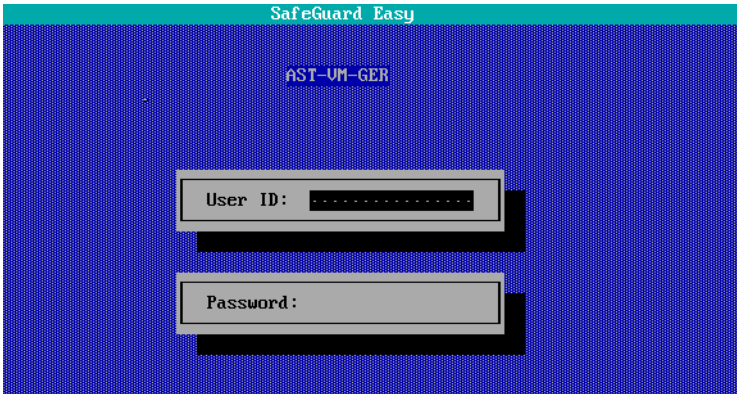


6. Select the "Replace the power-on and hard drive passwords with the fingerprint reader" check box.
7. Install SafeGuard Easy.
8. In the configuration settings, select **General/Authentication/Logon**, and then the "Fingerprint" option.
9. Restart the PC.

10. After this, swipe your enrolled finger over the reader.



11. The system displays the pre-boot authentication screen. However, you are not prompted to enter any information: the system only displays the text "Start authentication via Fingerprint reader (press any key to continue)".
12. You now see the fingerprint logon. Now swipe the finger you want to link to the SafeGuard Easy data over the reader. You must already have enrolled this finger with the ThinkVantage fingerprint software!
13. The system displays the pre-boot authentication screen. Now enter the SafeGuard Easy access data that is to be used for authentication together with the fingerprint.



14. Press [F6] to link another finger with the SafeGuard Easy access data in case the first one is not recognized, for example, if you have injured it.

15. You have now created the link with your fingers. Now, each time you restart your PC or notebook, you only need to swipe the enrolled finger to log on to SafeGuard Easy and Windows.

NOTES:

You can also press [Esc] to interrupt the fingerprint logon process and log on using your SafeGuard Easy user name and password instead.

You will need to interrupt this process by pressing [Esc], if

- although fingerprint authentication is installed, no fingerprint reader has been connected to the PC or notebook
- the user cannot log on using their fingerprint or if there is a problem with the fingerprint reader. Press the [Esc] key to return to pre-boot authentication. There the user can log on as usual with their SafeGuard Easy user name and password.

16.4 Changing the SafeGuard Easy password

Users can change their password

- in the pre-boot authentication phase.
- in SafeGuard Easy administration.

To change your password in the Pre-boot authentication phase:

1. Start the PC. The fingerprint logon appears.
2. Press [Esc] The system displays the pre-boot authentication screen.
3. Enter your SafeGuard Easy access data.
4. Press [F10] and change your password.
   The PC now starts without prompting you to enter your fingerprint.
5. Restart the PC. You now see the fingerprint logon.
6. Swipe your finger over the reader. The system displays the pre-boot authentication screen.
7. Enter your user name and the new password
8. Press Enter to confirm this. The fingerprint logon appears.
9. Swipe your finger over the reader. This links your SafeGuard Easy data to your finger and the logon procedure continues.

You have now reset your password.

To change the password in SafeGuard Easy Administration:

1. Start the Administration system by selecting the Programs/Utimaco/SafeGuard Easy/Administration menu option.
2. Select the "Users" folder and change your password in "Configure Password".
3. Restart the PC. You now see the fingerprint logon.
4. Swipe your finger over the reader. The pre-boot authentication now appears with the message that data does not match up.
5. Enter your SafeGuard Easy access data (new password!). You are now logged on.

Your new SafeGuard Easy access data has now been linked with your fingerprint.

16.5 Frequently asked questions

Do I need additional software, such as Lenovo's Client Security Solution (CSS)?

SafeGuard Easy's fingerprint solution runs independently of CSS. You only need the ThinkVantage Fingerprint Software to enroll your fingers.

How many users does it support?

Each reader has space for 21 fingerprints. Every one of these fingerprints can be assigned to a Windows user by using the ThinkVantage Fingerprint Software. It functions in the same way with SafeGuard Easy. The only difference is that the fingers and the SafeGuard Easy user data are linked during pre-boot authentication (for example, you can use your left-hand index finger to log on as the SYSTEM user and your right-hand index finger to log on as the USER).

What happens if the fingerprint logon does not work (because the device is defective)?

You can press [Esc] to return to pre-boot authentication and log on with your SafeGuard Easy user name and password. If you do not remember your password, use the challenge/response procedure to have a new one assigned to you.

17 Configuring Windows logon

During Pre-Boot Authentication (PBA) SafeGuard Easy requires authentication as its first system component. The usual Windows logon dialog is not displayed until the system has been unlocked using valid SafeGuard Easy data.

However, users often find it annoying to have to remember different passwords just to gain access to their PC. As a result, they may sometimes write down these different passwords so that they can remember them. This of course poses a considerable risk to company security. In larger networks forgotten passwords also cause extra work and costs for help desks.

This is why SafeGuard Easy provides Secure Automatic Logon and password synchronization functionality to take the burden of multiple authentication off users. Now, they only need to enter their user data once, during PBA. The administrative template includes a range of other options that can be used to make Windows logon even more user-friendly.

17.1 Secure Automatic Logon (SAL)

Automatic logon is a function that helps make the logon procedure more user-friendly. A user only needs to enter their Windows logon data once. In future logons, they automatically log on to Windows, and the user then only needs to use SafeGuard Easy user data to authenticate themselves during PBA. SafeGuard Easy calls this logon procedure **Secure Automatic Logon** or **SAL** for short.

SAL can be performed with or without a smartcard. You can choose which, while installing SafeGuard Easy.

Logging on to the operating system automatically is optional and can be switched off later with the SafeGuard Easy command `Chgsal.exe`.

WARNING:
You must install **either** SAL **or** logon using a smartcard.

All subsequent logons to other applications must be carried out manually.

Logon to Novell is only supported when smartcards are used.

During the installation of Windows, if the "Always logon this user" option is selected, SAL cannot be performed.

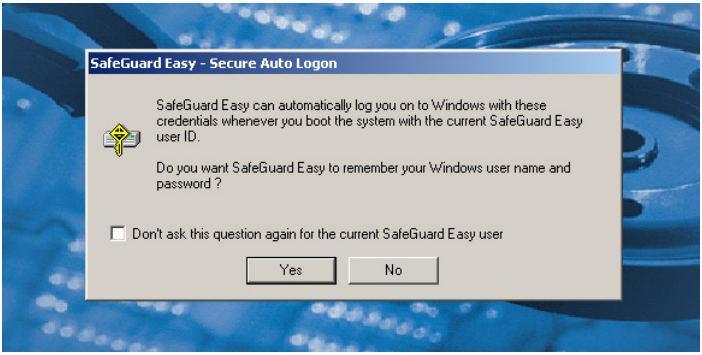
17.1.1 Installing Secure Automatic Logon (SAL)

In technical terms, SAL works like this: a user uses their SafeGuard Easy access data to log on during PBA and then enters their Windows user data in the Windows logon screen. SAL creates a relationship between the SafeGuard Easy user who has logged on and the Windows user, and stores it in an encrypted file called `SGSAL.dat`. The file is stored at <*system drive*>`\SYSTEM32`. When the user logs on to PBA again, SAL automatically passes the Windows user data on to the Windows logon screen, without user interaction.

How to configure SAL:

1. Install SafeGuard Easy with
   - "Secure Automatic Logon".
     Warning: do not install the option "SmartCard Auto Logon"!
   - Pre-Boot Authentication (Option "Password at system start")
2. Restart your computer.
3. Authenticate yourself in PBA with the SafeGuard Easy user data.
4. After logon, the familiar Windows logon dialog is displayed, if this is the first time you have ever logged on, after SAL has been installed.
5. Enter the correct logon information in the input fields and click [OK].

6. You then see the SAL dialog.


SafeGuard Easy - Secure Auto Logon
SafeGuard Easy can automatically log you on to Windows with these credentials whenever you boot the system with the current SafeGuard Easy user ID.
Do you want SafeGuard Easy to remember your Windows user name and password ?
Don't ask this question again for the current SafeGuard Easy user
Yes
No

[Yes]: Activates the relationship between the SafeGuard Easy and the Windows user.

[No]: Does not use SAL functionality.

The status of the check box labeled "Don’t ask this question again for the current SafeGuard Easy user" specifies whether the dialog is to be displayed again on every logon or not.

7. Click [OK] and select the check box.

8. This associates the SafeGuard Easy user with the Windows user. Next time the PC is restarted, and the user enters their SafeGuard Easy user data during PBA, they are automatically logged on to Windows.

Changing the Windows password

Windows passwords have to be changed regularly for security reasons. However, the way in which a newly-defined password is integrated into the Secure Auto Logon process depends on the method used to change the user password.

- **Forced Password Change**
  Users can be forced to change their operating system passwords by the "User must change password after next logon" option in their user profile. If the user has to change their password when logging on, they are prompted to do so by a system message. SAL is deactivated for this logon.

  You must confirm the system message by clicking on [OK]. The following dialog requires the user to enter a new password. As soon as the user confirms the new password, the system updates the SAL file. At next logon, the user can log on without having to re-enter their Windows access data, and Secure Auto Logon is run without notification.

- **User Changes Password**

  - If the user change the password in the **Windows logon dialog** (e.g. by pressing [CTRL]+[ALT]+[DEL] on their desktop), they can change their password by selecting "Change password". If they change their password in this way, the system **automatically accepts the new Windows password**, and stores it in the `Sgsal.dat` file. When logging on after a password change, the user does not have to re-enter their Windows access data, and Secure Auto Logon is run without notification.
  - If the password is changed via **Windows user administration**, the system **does not automatically accept the new Windows password** and it is not stored it in the `Sgsal.dat` file. Instead a warning message appears on the screen saying that the Windows password is not valid and the user must enter the correct new one in the logon screen. After the password has been changed, the user can log on without having to re-enter their Windows access data, and SAL is run without notification.

17.1.2 Secure Automatic Logon with smartcard (Smartcard SAL)

The Smartcard SAL function stores the PIN on the card in such a way that the smartcard is automatically released when the user enters their SafeGuard Easy data during PBA. The smartcard then reads the Windows logon data (provided that it is saved on the card) and the data is then used to log on to the operating system.

How to implement Smartcard SAL:

1. Install SafeGuard Easy.
   - Select the "SmartCard Auto Logon" option.
     Warning: Do not install the "Secure Auto Logon" option!
   - Install the "Password at system start (PBA)" option.
2. Restart your PC so that the PBA dialog appears.
3. During PBA, enter your SafeGuard Easy User ID and Password.
4. Insert your smartcard in the smartcard reader. You see the PIN entry dialog. Enter your personal PIN in the dialog.
5. If no Windows information is saved on the smartcard, the system displays a dialog that prompts you to confirm whether the data should be written to the smartcard. If you click "Yes", you see the "Windows Access Data" dialog. In it you can enter your User Name, Password and Domain, which will be written to the smartcard.

> ***NOTE:***
> The Windows user written to the smartcard must already have been created on the operating system, otherwise the logon will not be successful.

6. The system displays a dialog, prompting you to confirm whether Smartcard SAL is to be enabled.
   Enable: [YES]
   Disable: [NO]

7. After you have entered the SafeGuard Easy User ID and Password during PBA, you will automatically log on to Windows, when the PC is restarted, provided that the smartcard is inserted in the reader.

Changing the smartcard PIN

You can change PINs with external SafeGuard tools such as the Token Administration.

If a user changes the smartcard PIN with this tool, this affects Smartcard SAL because the PIN stored on the smartcard no longer matches the PIN stored in the `Sgsal.dat` file. If the PC is restarted, the system stops at the PIN entry dialog. The user is prompted to enter the correct PIN. After the user enters the "new" PIN, they log on and the "new" PIN is stored in the `Sgsal.dat` file.

17.1.3 Switching Secure Auto Logon off temporarily

If Secure Auto Logon (with or without smartcard) is enabled, it can be disabled later, by a user with Windows administrator rights, and enabled again by running `CHGSAL.EXE` from the SafeGuard Easy directory.

To do so, proceed as follows:

1. Boot in MS DOS mode or select the Run command in the Windows Start Menu, and then run "cmd" to display the DOS prompt.

2. Switch to the directory in which SafeGuard Easy is stored (e.g. on a network drive). Enter the following command with the appropriate parameters:

```
CHGSAL.EXE /SAL:ON | /SAL:OFF | /SCSAL:ON | /SCSAL:OFF | [ /? ]
```

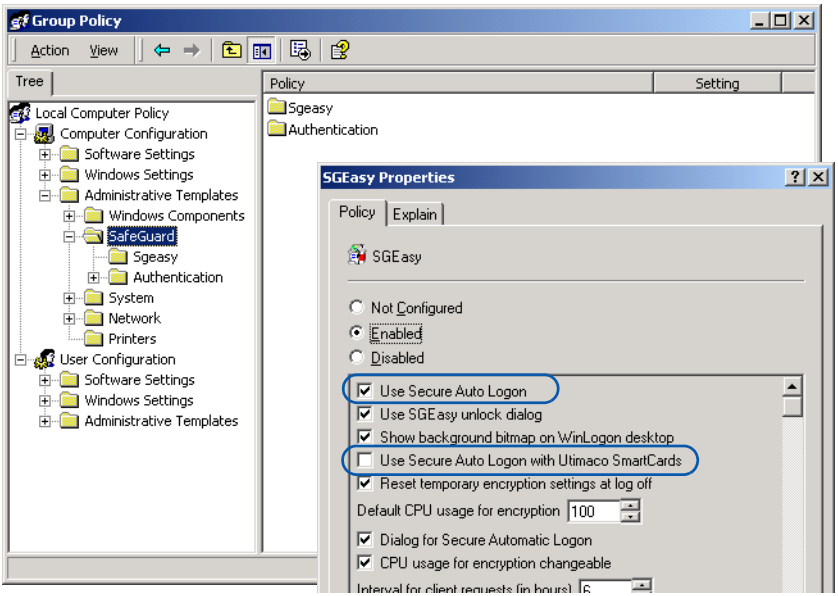
/SAL:ON	Enable Secure Auto Logon
/SAL:OFF	Disable Secure Auto Logon
/SCSAL:ON	Enable Smartcard SAL
/SCSAL:OFF	Disable Smartcard SAL
/?	Summary help

This tool only works if SafeGuard Easy is installed with SAL or Smartcard SAL.

You can also toggle SAL and Smartcard-SAL via a policy in Utimaco's administrative template. You will find the policy in

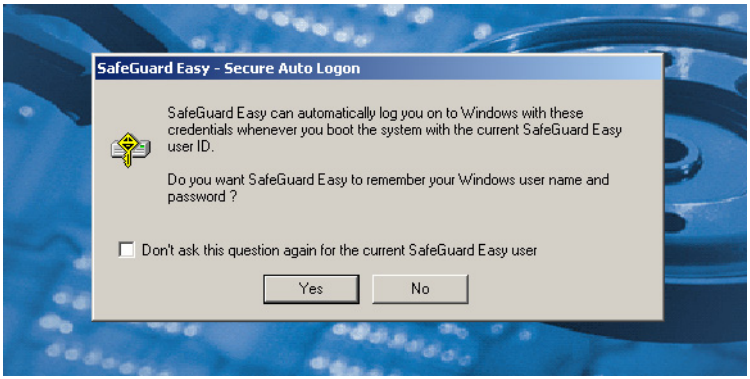
Computer Configuration
\Administrative Templates
\SafeGuard
\SGEasy

In the Features menu, simply add or remove the checkmark for "Secure automatic logon" or "Secure automatic logon with smartcards".



17.1.4 Hiding the SAL dialog

The SafeGuard Easy SAL function automatically logs users onto the operating system. The user activates the SAL via a dialog prompt.

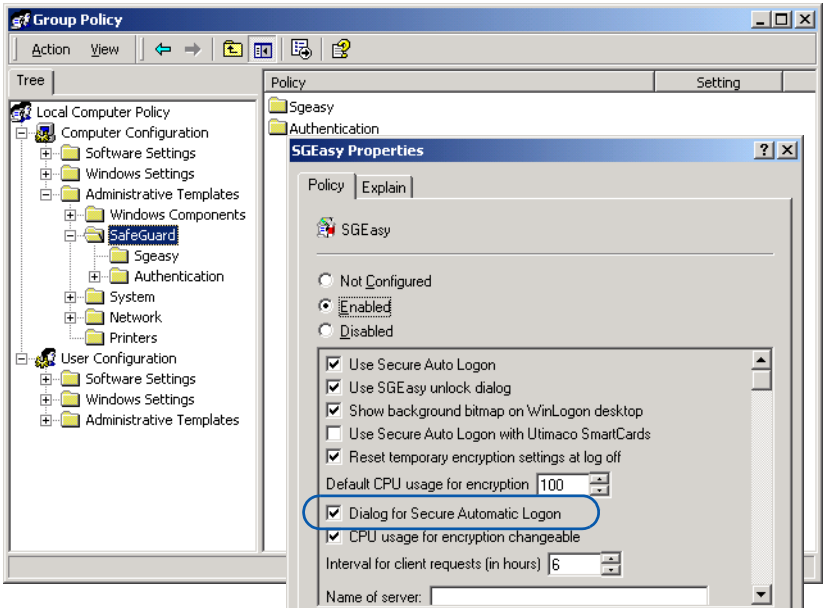

SafeGuard Easy - Secure Auto Logon
SafeGuard Easy can automatically log you on to Windows with these credentials whenever you boot the system with the current SafeGuard Easy user ID.
Do you want SafeGuard Easy to remember your Windows user name and password ?
Don't ask this question again for the current SafeGuard Easy user
Yes
No

To prevent users from refusing automatic Windows logon, SafeGuard Easy can suppress this dialog for all SafeGuard Easy users, if required, and run the SAL without a prompt.

You can hide the SAL dialog via a policy in Utimaco's administrative template. The policy is available at

Computer Configuration
\Administrative Templates
 \SafeGuard
  \SGEasy

In the Features menu, simply add or remove the tick for "Dialog for secure automatic logon".



17.1.5 Removing data for SAL/SCSAL

If you delete `Sgsal.dat` (<System drive>\SYSTEM32), all saved user data is also removed. After you restart the computer you can assign new data to a SafeGuard Easy user.

If a SafeGuard Easy user, who has already established a connection, is deleted on a system, this connection continues to exist when the same user is created again.

17.1.6 Restriction

SAL is temporarily switched off if a user logs on with the "One-time logon" option. One-time logon allows a user to log on to SafeGuard Easy in the Pre-Boot Authentication (PBA) even if he/she does not know the SafeGuard Easy user credentials, provided the Challenge Code and Response Code were exchanged successfully (see 'Remote maintenance (Challenge/Response)').

If a user is granted a "One-time logon" at PBA level, they are not automatically logged on to Windows - even if SAL is enabled. The operating system stops, the familiar Windows Logon dialog appears and they must enter their Windows user credentials manually. Every action performed at the PC is then recorded with the name of the logged on Windows user.

After a "normal" logon with valid SafeGuard Easy credentials at PBA level, SAL and automatic Windows logon is performed in the usual way.

17.2 Logging onto Windows and SafeGuard Easy using the same password (password synchronization)

The SafeGuard Easy "password synchronization" function helps to reduce the possibility of passwords being forgotten because it makes the password for SafeGuard Easy identical to the Windows password.

As a result, users only need to remember one password (i.e. for Windows) to log onto both SafeGuard Easy and the operating system.

If secure automatic logon (SAL) is also switched on, a user only needs to enter their (Windows) password in Pre-Boot Authentication (PBA) and the Windows logon is performed automatically.

Password synchronization also has mechanisms that ensure that the SafeGuard Easy password and the Windows password will remain identical.

By default, password synchronization is switched off. You need a registry key to activate it.

17.2.1 Benefits of password synchronization

- Users only need to remember one password (the Windows password).
- The helpdesk only has to manage one password per user.
- It is no longer necessary to administer SafeGuard Easy and Windows rights in parallel. If configuration allows, password policies are controlled solely via Windows policies.

17.2.2 Preparing for password synchronization

How to prepare password synchronization:

1. Activate "Secure Automatic Logon" (SAL).

   Necessary if the SafeGuard Easy User name and Windows User name are different.
   Not necessary if the SafeGuard Easy User name and Windows User name are the same.

2. Activate Pre-Boot Authentication.

3. Modify SafeGuard Easy password rules.

   If you are using password synchronization, we recommend that you switch off all SafeGuard Easy password rules!

   If the SafeGuard Easy password rules are not switched off they may interfere with Windows account rules and cause inconsistencies.

   > ***NOTE:***
   > You must make the following setting in SafeGuard Easy:
   > Minimum age of passwords = 0

4. Switch on password synchronization.

   Set the “PasswordSync” registry key as described and reboot the PC.

5. Activate SafeGuard Easy Logon feature (Utimaco Master GINA).
   In a standard SafeGuard Easy installation the Utimaco Master GINA is always installed and does not need to be activated again.
   However, password synchronization cannot be used if Utimaco Master GINA has been specifically deactivated as part of a central distribution of SafeGuard Easy.

17.2.3 Switching on password synchronization

To activate password synchronization, you must make changes to the Windows Registry database. Use the registry editor ("regedit") or central mechanisms to edit this Registry database.

After you open the registry editor, in the registry key

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
Sgeasy

create the DWORD value "**PasswordSync**".

To activate password synchronization, change the value of "PasswordSync" from 0 (switched off) to 1 (switched on).

Now close the Registry and restart the PC.

17.2.4 Carrying out password synchronization

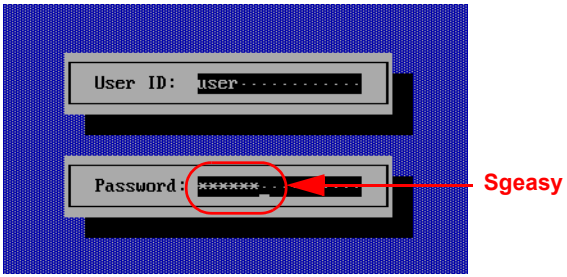
1. Make all the preparations for password synchronization.

   Do not forget this SafeGuard Easy setting:
   Set the "Minimum age for passwords" to "0".

2. Restart the PC.

3. The SafeGuard Easy logon screen (PBA) appears. Enter SafeGuard Easy user data, for example

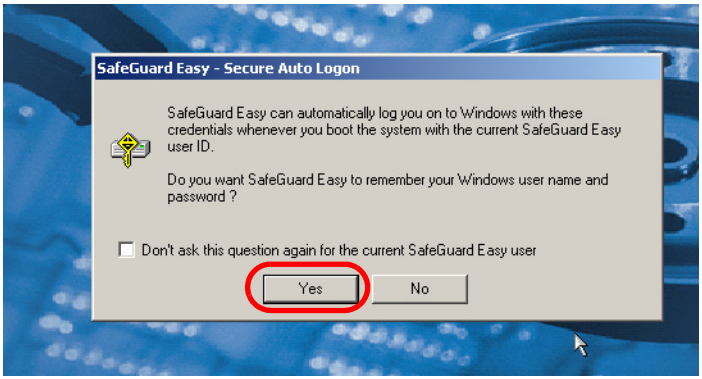
   SGE user name: **User**
   SGE password: **Sgeasy**



4. The Windows logon screen is displayed. Enter Windows data, for example

   Windows User Name: **AMiller**
   Windows Password: **WinSecurity**

5. The SAL dialog is displayed. Click [Yes] to confirm.


SafeGuard Easy - Secure Auto Logon
SafeGuard Easy can automatically log you on to Windows with these credentials whenever you boot the system with the current SafeGuard Easy user ID.
Do you want SafeGuard Easy to remember your Windows user name and password ?
Don't ask this question again for the current SafeGuard Easy user
Yes
No

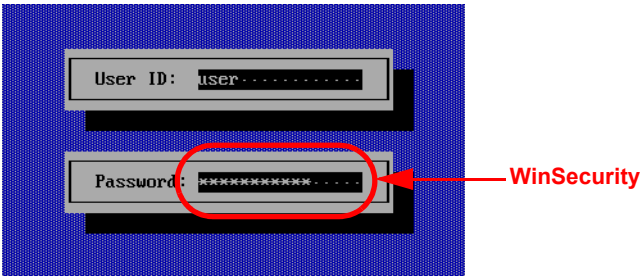
6. The system displays the password synchronization dialog. In it you are prompted to enter the SafeGuard Easy password (in our example "**Sgeasy**"). If you enter the correct password SafeGuard Easy "allows" the passwords to be synchronized. Click [OK] to confirm.

7. The system displays the Windows desktop.

8. Restart the PC.

9. PBA appears. Enter the SafeGuard Easy user data.

   SGE user name: **User**
   SGE password: **WinSecurity (= Windows password)**



10. The PC boots (you no longer need to log onto Windows!)

11. The system displays the Windows desktop.

17.2.5 Changing the Windows password when password synchronization is active

WARNING:
The Windows password rules will apply to the new password and not the SafeGuard Easy rules!

1) User changes their Windows password locally in the Windows security dialog (Ctrl]+[Alt]+[Del])

Result: the new Windows password applies immediately to both Windows and SafeGuard Easy.

2) Administrator changes Windows passwords either centrally or via remote administration

Result: the new password applies to Windows, but not to SafeGuard Easy!

In this way the "old" SafeGuard Easy password and the "new" Windows password can be resynchronized:

1. After a restart the user enters the old password at PBA.

2. The automatic Windows logon fails because the SafeGuard Easy password and the Windows password have not yet been synchronized. As a result the user is prompted to enter their new Windows password in the Windows logon screen.

3. The SAL dialog is displayed and must be confirmed again by clicking [Yes].

4. The system displays the password synchronization dialog. Synchronization takes place after the "old" password has been entered.

5. After restarting the PC the user uses their new (Windows) password to log on at PBA.

17.2.6 Changing the SafeGuard Easy password

Password synchronization means the current Windows password is always used as the password for SafeGuard Easy.

For this reason, We recommend that you do not change the SafeGuard Easy password. Instead, we recommend that you use the familiar Windows mechanisms for changing the password.

However, if circumstances require you to change the SafeGuard Easy password, the new password is subject to the password rules as defined in SafeGuard Easy Administration.

17.2.7 Cancelling the password synchronization dialog

You can toggle the registry key to define whether the password synchronization dialog can be cancelled without making an entry. This setting can be used, by administrators for example, to force users to carry out password synchronization.

After you open the registry editor, in the registry key

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
Sgeasy

create the DWORD value "**ForcePasswordSync**".

If you enter the value "1" the "Cancel" button is shown in gray and users cannot continue until they have completed the synchronization dialog. If you enter the value "1" this allows users to jump over the dialog.

Now close the Registry and restart the PC.

17.2.8 Restrictions

SafeGuard Easy restricts passwords to 16 characters
At logon during PBA, SafeGuard Easy will only accept passwords with a maximum of 16 characters. SafeGuard Easy itself defines this rule and it cannot be changed. If a synchronized Windows password is too long the "excess" characters will be "cut off" for authentication in SafeGuard Easy (PBA, Administration etc.).

Example:
Windows password (20 characters): "UtimacoSecurity12345"
Logon during PBA (16 characters): "UtimacoSecurity1"

Synchronization does not take place if the Windows password

- does not comply with SafeGuard Easy's internal password rules (see 'Pre-defined password rules')
- is present in the SafeGuard Easy password history
- contains specific special characters

  Permitted characters are:
  Characters that are created with one keystroke or in combination with the SHIFT key, e.g. ! " § $ % &/( ) = ? * ' ; : -
  The following characters are not permitted:
  characters that are created using the [ALT Gr] key, for example ² ³ { [ ] } \ ~ @ € | µ é è ê (and all other letters with accents)

> ***NOTE:***
> Some keyboard layouts allow you to create a special character with one keystroke or in combination with the SHIFT key, for example the characters with accents on a French keyboard. In this case the special character is supported by SafeGuard Easy's password synchronization.

Additional restrictions when password synchronization is active:

- No more than 16 Windows users permitted per machine (16 = maximum number of SafeGuard Easy users).
- Password synchronization with the token is only possible if the token remains inserted while the password is being exchanged.

17.2.9 What should I do, if ...

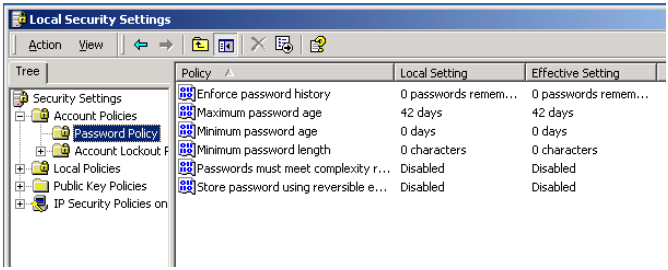
... password synchronization fails and an error message appears?
This may happen because:

- The synchronized password does not comply with SafeGuard Easy's password rules (for example, it is too short).
- The synchronized password contains invalid characters or special characters that are not supported by SafeGuard Easy.
- According to SafeGuard Easy's password history, the synchronized password has already been used.

How to resolve the problem:

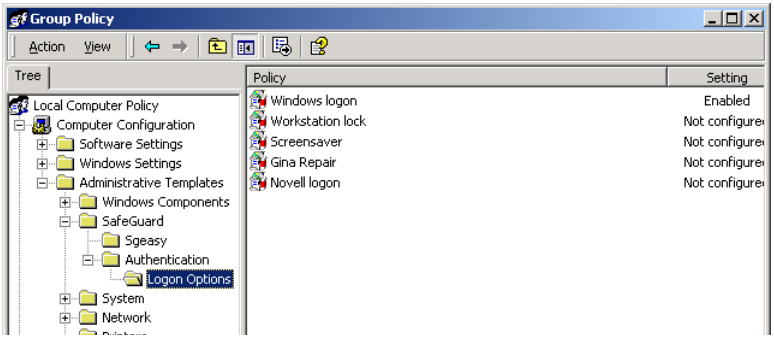
Define a new synchronized password that does not infringe the Windows or SafeGuard Easy rules.

... you do not know how the policies for the synchronized password (=Windows password) have been defined?
In the Windows Start menu, go to **Settings/Control Panel/ Administrative Tools/Local Security Settings**. All possible settings are listed under Account policies > Password Policy.



17.3 Additional Windows Logon options

You can use the Sguard.adm administrative template to predefine settings concerning Windows logon via group policies. Additionally it is possible, for example, to set screen saver options which normally cannot be influenced with the regular Windows settings.



17.3.1 Tailoring the Windows Logon screen

These settings define the desktop view, which is displayed at logon/logoff and when the workstation is locked.

You will find the policy in the administrative template at

Computer Configuration
\Administrative Templates
\SafeGuard
\Authentication
\Logon Options
\Windows logon

- **Use Utimaco logon dialog**
  If you select this check box, the Utimaco logon dialog appears at logon. If you deselect this check box, you can log on to the system using the Windows logon dialog.

- **Use Utimaco start dialog**
  If you select this check box, the SafeGuard Logon dialog is displayed when the PC boots. You are prompted to press [Ctrl]+ [Alt] + [Del] to open the logon dialog. If you deselect this check box, the appropriate Windows logon dialog appears.

- **Use Utimaco lock dialog**
  During workstation lock with [Ctrl] + [Alt] + [Del], the SafeGuard lock dialog will be displayed instead of the Windows dialog. If an invalid user logon has been registered, it will be displayed within the Utimaco lock dialog.

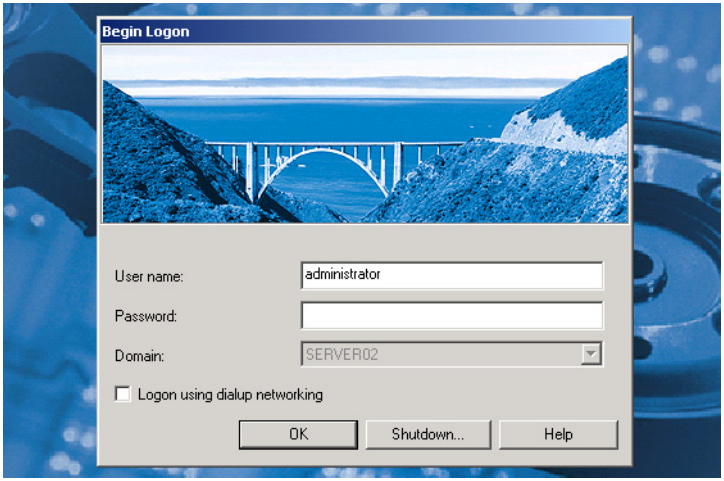
- **Disable precheck of user data with RAS**
  If you select this check box, the system performs no preliminary check of user accounts when establishing RAS connections.

- **Enable locked logoff**
  If you select this check box, you allow users of a locked workstation to undo a PC lock caused by another user who has removed their token. The PC lock is removed after the user has logged on.

- **Disable check box for RAS logon in Utimaco logon dialog**
  Defines if the "Logon using Dialup Networking" check box is automatically disabled or not, in the Utimaco logon screen.

- **Display SafeGuard Plug-in in 3rd party logon dialog**
  If activated, a note saying that SafeGuard Authentication is installed is also displayed in a 3rd party logon dialog.

- **Replace bitmap with**
  In this edit field a bitmap, which is displayed in the logon dialog, can be specified. for example a company logo to a suitable background. The bitmap must be in .bmp format, and must reside in the System32 folder of the Windows installation folder. The size of the bitmap is 413x140 pixel.



17.3.2 Workstation lock

Workstation lock sets how many login attempts a user can make before the PC is locked, and how the time delay between these login attempts increases. The mechanism only works for local users who are not members of the local administrator group.

You will find the policy in the administrative template at

Computer Configuration
\Administrative Templates
\SafeGuard
\Authentication
\Logon Options
\Workstation Lock

The mechanism only applies for users who are not members of the local administrator group. For restrictions related to Terminal Server usage see chapter *Terminal Server Support*.

- **Logon Attempts**
  In this field you set the number of logon attempts a user can make with an invalid user name or password. If you enter "3", for example, the PC will be locked if the user enters their user name or password incorrectly three times in a row, when logging on.
  Minimum/maximum values: 0-999

- **Delay in Seconds**
  Enter the base value here. The base value is the figure which, multiplied by the multiplier, is used to calculate the waiting time after the first unsuccessful logon attempt. If there is another unsuccessful logon attempt, the waiting time of the previous attempt is taken as the base value. Default value is 10.
  Minimum/maximum values: 0-999

- **Multiplier**
  The Multiplier is multiplied by the Delay in seconds value. The default value is 3.
  Minimum/maximum values: 0-99

- **Disable CTRL+ALT+DEL when workstation is locked**
  Workstation remains locked after the user presses CTRL+ALT+DEL.

Example:

The delay is 10 sec. and the multiplier is 5 sec:
1st unsuccessful attempt: 50 seconds waiting time (10 x 5)
2nd unsuccessful attempt: 250 seconds waiting time (50 x 5)
3rd unsuccessful attempt: 1250 seconds waiting time (250 x5)

NOTE:

The lock can be deactivated

- by rebooting the PC
- when a local administrator logs on
- by data replication from the domain controller
  In this context, also note the Windows user lock.

17.3.3 Screen saver

You can specify the system's reaction if a screen saver is switched on. To do so the Windows screen saver must be enabled!

You will find the policy in the administrative template at

Computer Configuration
\Administrative Templates
\SafeGuard
\Authentication
\Logon Options
\Screensaver

- **Action**
  Under *Action* you can define the following reactions when a screen saver runs. These actions may cause different effects, depending on where they are set (local workstation or for terminal server sessions). To define these actions for terminal server sessions, you must set them on the terminal server:

  A) Logoff user:
  The current user will be logged off the machine. Other users registered on the workstation or within the network are now able to log on to the workstation.

  B) Shut down the workstation:
  The workstation will automatically shut down and has to be rebooted for another logon.
  In a terminal server sessions the user will be logged off.

  C) Restart the workstation:
  The workstation will be automatically restarted.
  In a terminal server sessions the user will be logged off.

  D) Hibernate the workstation
  The computer is hibernated.
  In a terminal server sessions the session will be locked.

NOTE:
If SafeGuard Advanced Security and SafeGuard Easy are installed on the same machine, this option works only when SafeGuard Easy Version 4.0 or higher is used.

E) Disconnect the session
Has no effect on a local workstation.
In a terminal server sessions the session is disconnected.

F) Standby
The computer is put on standby.
In terminal server sessions, the session will be locked.

Possible actions and their effect on the local workstation or in a terminal server session:

Setting	Action local or on Server	Action in Terminal Server Session
<None>	no action	no action
Logoff user	logoff	logoff
Shut down the workstation	shut down	logoff
Restart the workstation	restart	logoff
Hibernate the workstation	hibernate	lock session
Disconnect the session	no action	disconnect session
Standby	Standby	lock session

NOTE:
In a **Remote Desktop session** for the settings the same actions apply as described under **local or on server**.

- **Delay (default 15 minutes)**
  “Delay“ defines the time after which one of the actions described above takes place. The default setting is 15 minutes. You can change the setting by clicking the entry field and using the keyboard, or with the direction arrows.
  Maximum/minimum values: 0-900
- **Disable Screensaver**
  Usually a screen saver is cancelled when the user moves the mouse or uses the keyboard. Afterwards a user can continue working without entering their user data. If the "Disable screensaver" check box is selected, the workstation is locked. Once the PC is locked, the only way to access the PC again is to enter the correct user data.

Example:

A workstation’s screen saver should be activated ten minutes after the last user action. If "Shut down the workstation" is selected as the action, and a 13 minutes delay is set, the PC will be automatically shut down 23 minutes after.

17.3.4 GINA repair

Utimaco uses its own logon component (SafeGuard GINA (`SGGINA.dll`)). After installation it is always the first Windows logon component called by the operating system.

The installation of any other product can change the position of the logon components.

You will find the policy in the administrative template at

Computer Configuration
\Administrative Templates
\SafeGuard
\Authentication
\Logon Options
\GINA Repair

- **Repair GinaDLL entry in registry when changed:**
  The "Repair GinaDLL entry when changed" option ensures that the SafeGuard GINA is automatically set as the first logon component called by the operating system.

- **Unknown Gina handling**

  Ask User
  When the GINA is initialized for the first time, a dialog opens in which the user is prompted to select the unknown or the original Microsoft GINA. If the check box "Don't show this message again" is selected, the user's choice is stored in the registry and this registry value is used after the system is rebooted.

  Use Original Microsoft GINA
  The original Microsoft GINA is used as the first logon component called by the operating system.

  Use unknown GINA
  An unknown GINA is used as the first logon component called by the operating system.

17.3.5 Novell logon

Can only be used in combination with SafeGuard Advanced Security's Single Sign On!

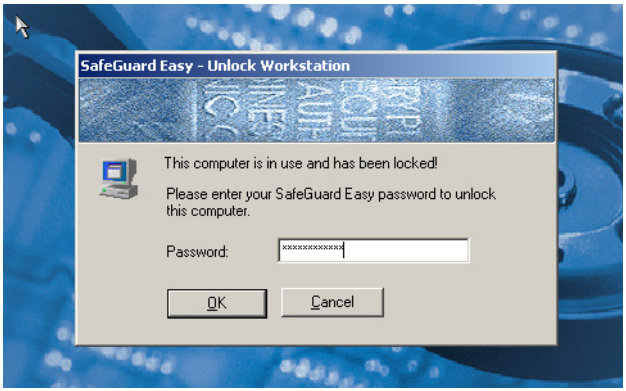
This rule helps SafeGuard Single Sign On to detect Novell logon dialogs if multi-language versions are in use. SafeGuard Single Sign On watches the default Novell dialog title and the logon dialog title entered here and completes them with Novell logon information which are stored on the token.

You will find the policy in the administrative template at

Computer Configuration
\Administrative Templates
\SafeGuard
\Authentication
\Logon Options
\Novell Logon

18 SafeGuard Easy workstation lock

SafeGuard Easy replaces the regular Windows workstation lock with its own dialog.


SafeGuard Easy - Unlock Workstation
This computer is in use and has been locked!
Please enter your SafeGuard Easy password to unlock this computer.
Password:
OK
Cancel

If the PC is in rest mode, only the user that locked it can activate the user interface again by entering their SafeGuard Easy password.

The screen and user interface lock:

- when you press [CTRL] + [ALT] + [Delete] and [Lock Computer].
- after a set time has passed without any user operations (wait time).
- when the user removes the token.

When the PC is in rest mode, the same background bitmap is displayed as during logon, but this can be changed (see 'Changing the background bitmap in the Windows logon dialog').

18.1 Prerequisites

The workstation lock only works if

- Pre-Boot Authentication is active.
- the user has logged on to the operating system automatically via SAL.
- the Windows screen saver with password protection is switched on.

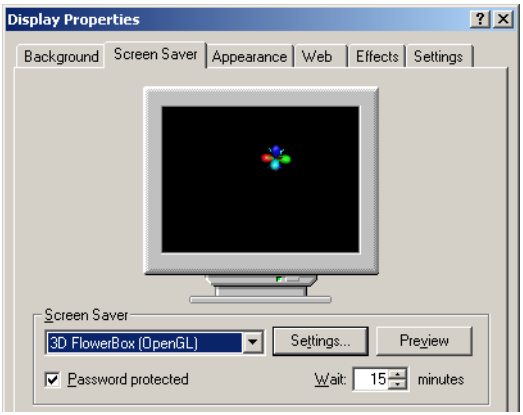
After activating the Windows screen saver settings you must reboot the PC.

The SafeGuard Easy workstation lock is switched off afterwards if a user logs off, and then logs on again, after successfully logging on to Windows.

18.2 Activating the Windows Screen Saver with password protection

You control the SafeGuard Easy workstation lock in the Windows settings in Start/Settings/Control Panel/Display/Screen Saver.

Restart your workstation after enabling the screen saver.



First you must select a screen saver. Then set the "Password protected" and "Wait" (wait time) options.

- **Password protected**
  Forces a prompt to enter the SafeGuard Easy password, must be activated.

- **Wait**
  Specifies the time (in minutes) that must pass without the workstation being used before the screen saver is switched on. If you set 15 here, for example, the screen will be switched off after 15 minutes without keyboard entry or mouse movements. The user must enter their SafeGuard Easy password again to continue working.

To protect the workstation against unauthorized users, we recommend you switch on the workstation lock.

18.3 Switching off the SafeGuard Easy workstation lock

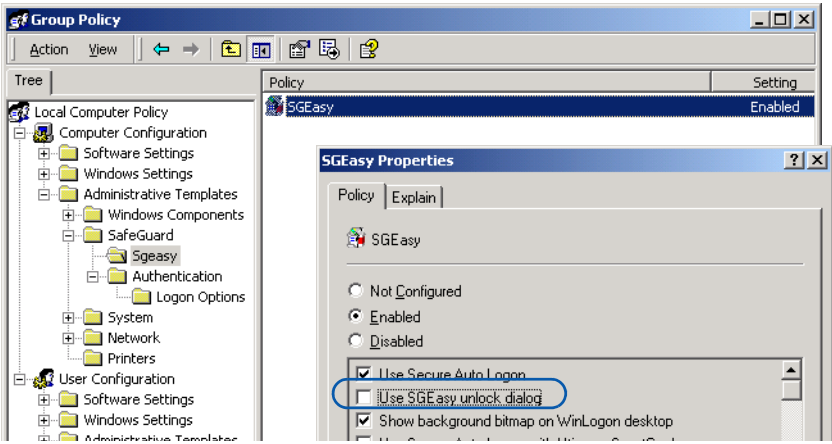
If you wish, you can switch off the SafeGuard Easy Workstation Lock and display the standard Windows dialog instead.

> ***WARNING:***
> The standard Windows dialog is not locked with the SafeGuard Easy password but with the Windows password. This means that SafeGuard Easy password protection is then no longer provided for Workstation Lock!

If the SafeGuard Easy-Workstation Lock is **NOT** to be displayed, you can configure this using the "Use Sgeasy unlock dialog" policy (deselect tick to the left of the policy).

You will find the policy in SafeGuard Easy's Administrative Template at

Computer Configuration
\Administrative Template
\SafeGuard
\SGEasy



19 Secure Wake-On-LAN

Secure Wake-On-LAN mode in SafeGuard Easy is the most secure way of combining the benefits of Wake-On-LAN with hard disk encryption to protect the PC. To do this, SafeGuard Easy's WOL allows Pre-Boot Authentication to be deactivated for a pre-defined number of restarts. After this it can be reactivated so that, for example, new software can be distributed. However, with WOL in use, it is not possible to use inactive PBA and attempt to sneak into the system using a Windows logon.

WOL is the best possible compromise between Pre-Boot protection and the performing of centrally-controlled tasks.

19.1 Overview

In general, Secure Wake-On-LAN allows any computer within a local network to be switched on by another computer in that network. This may happen so that new software updates can be loaded or to carry out routine maintenance tasks.

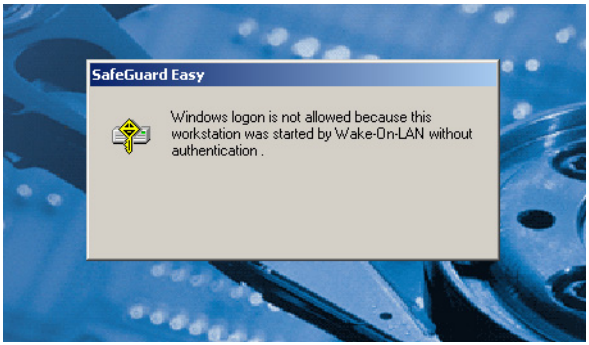
Unfortunately, it was not possible to use this user-friendly method of carrying out central tasks on computers secured with versions of SafeGuard Easy earlier than version 4.0, because of Pre-Boot Authentication (PBA). This is because the computer halted on PBA (if present) and expected the user to enter their SafeGuard Easy user data. If this happens, the operating system fails to boot and therefore does not create a network link. As a result, centrally-controlled tasks are simply not performed.

With the new WOL technology in SafeGuard Easy, administrators can allow SafeGuard Easy clients to have a pre-defined number of restarts before Pre-Boot Authentication automatically becomes active again. For example, if the number of automatic logons is set to "3", the PC can be booted three times one after the other with PBA switched off. The fourth time the PC is booted, PBA is automatically displayed again (provided that it is active).

During these automatic logon boot phases, the Windows logon dialog is not displayed. The computer boots automatically and the automatic software update can be carried out over the network.

19.2 Locking the Windows Logon

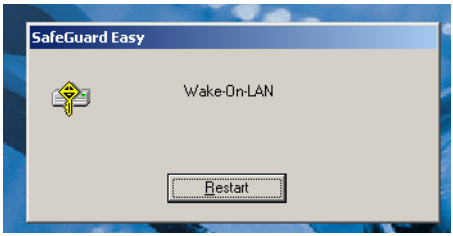
In Wake-On-LAN mode, the computer is protected against local Windows user logons. Instead of the familiar Windows logon dialog, the system displays the Wake On LAN dialog (“Windows logon is not allowed because this workstation was started by Wake On LAN without authentication.”)


SafeGuard Easy
Windows logon is not allowed because this workstation was started by Wake-On-LAN without authentication .

However, the Windows logon lock in WOL mode only works if SafeGuard GINA (Utimaco Master GINA) is installed!

19.3 Adjusting WOL dialog

The WOL message box (“Windows Logon is not allowed ...”) can be adjusted centrally by standard Windows mechanisms (registry keys).



Inserting Restart button

A "Restart" button is inserted if this registry key [DWORD] is set to "0":

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy
WOLDisableShutdown

Changing message text

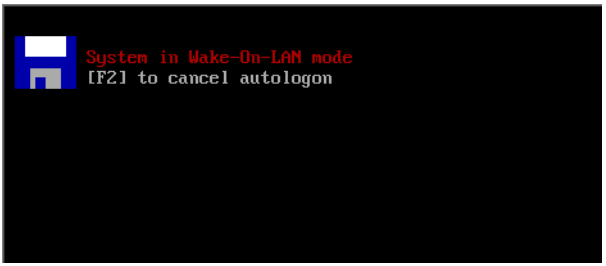
A new message box text can be entered under the following registry key [STRING]:

HKEY_LOCAL_MACHINE
Software
Utimaco
SGEasy
WOLNotice

19.4 Temporary removal of Wake-On-LAN locks

If, despite WOL mode, a user has to use their PC, there is a way to temporarily remove the lock:

In the Pre-Boot phase, a diskette icon appears for about 5 seconds in the top left-hand corner of the screen.



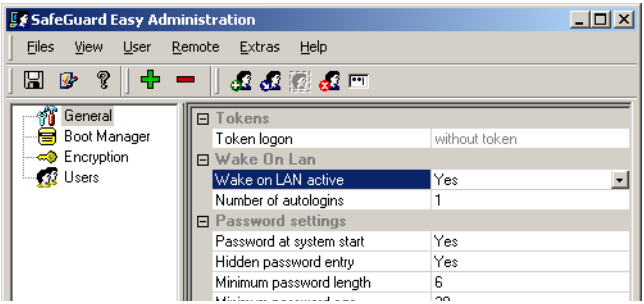
If the user presses [F2] during these 5 seconds, the PBA dialog is displayed and they can log on as usual with valid SafeGuard Easy data and then log into Windows. A flashing warning [F2] tells the user that the computer is in Wake-On-LAN mode.

If the PC is booted via secure mode (press [F8] during the boot procedure), the installed SafeGuard lock ensures that only users with Windows administrator rights can log on in secure mode.

19.5 Configuring Wake-On-LAN

WOL is usually installed in larger IT environments, not for stand-alone PCs. The administrator creates a configuration file that contains the relevant WOL settings and distributes them to the clients in the company.

You configure SafeGuard Easy's Wake-On-LAN feature in the administration programs on the "General" configuration page.



You can make the following settings:

- **Wake on LAN active**:
  Switches Wake-On-LAN mode on and off.

- **Number of autologins** (default: 1):
  Defines the number of restarts with deactivated PBA, if Wake-On-LAN is active.

  Utimaco always recommends **that one reboot more than necessary is permitted** so that unforeseen problems can be avoided.

As soon as the configuration file has been distributed to the user PCs, each PC now boots for this pre-defined number of times without PBA. After this pre-defined number of boots without PBA has been exceeded, the Pre-Boot Authentication dialog is displayed in the usual way and the user must enter the correct SafeGuard Easy user data.

20 Hibernation

Users with mobile devices frequently use the Windows "hibernation" function so that they can temporarily interrupt their working processes. If a notebook with active "hibernation" is shut during an operation, it automatically switches itself off. The next time it reboots it returns to exactly the same screen as it left off.

SafeGuard Easy has a special solution for securing data in hibernation mode that you will not find in many other encryption products.

20.1 Overview

In hibernation mode, the contents of the working memory (RAM) are written to the Hiberfile.sys system file in the root directory of the operating system partition (usually the C: drive), and stored on the hard disk. Hiberfile.sys is approximately the same size as the amount of available RAM. The computer is then switched off. The next time you switch on the computer, the desktop is exactly the same as it was when you shut it down (i.e. the contents of Hiberfile.sys are loaded back into RAM). If hibernation mode is deactivated, Hiberfile.sys becomes invalid.

20.2 Hibernation and SafeGuard Easy

In an unencrypted operating system partition switching a computer to hibernation mode is a security risk because this reallocates the entire contents of the RAM, which are then easily accessible to unauthorized outsiders.

In an encrypted operating system partition SafeGuard Easy enables the use of the hibernation feature because the generated Hiberfile.sys is encrypted and can therefore be stored securely on the hard disk. As a result, all the data on the hard disk is encrypted all the time. The system can only be accessed by users who can authenticate themselves by entering valid SafeGuard Easy data in PBA (if this is active) when the computer is rebooted.

NOTE:
If different SafeGuard Easy users are sharing one workstation, each of them can access the profile of the SafeGuard Easy user who initiated hibernation mode after they have authenticated themselves with their various SafeGuard Easy data in the PBA.

In this case a Windows password can be requested when the computer reboots ("Windows Control Panel Power Options/Advanced tab, Prompt for password when computer resumes from standby" check box). This setting requires each user to enter their Windows data as well when they log on (disadvantage: repeated authentication).

20.3 Prerequisites and restrictions

The interplay between SafeGuard Easy and the hibernation function is subject to the following prerequisites:

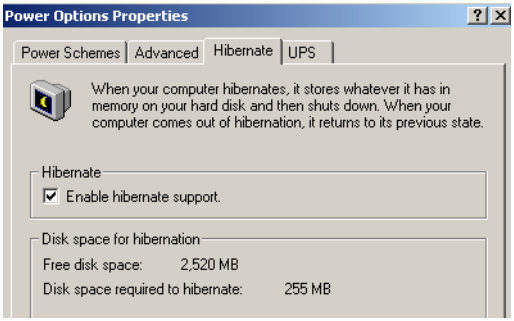
Hibernation with SafeGuard Easy supports ...	Hibernation with SafeGuard Easy does NOT support...
Windows 2000 and Windows XP	
hard disk drives (Microsoft IDE, Serial-ATA, SCSI) that are using Microsoft's default interfaces; if no default interfaces are used Serial-ATA can cause problems with some devices.	Hard disk drivers from third-party suppliers.
SafeGuard Easy encryption modes "Full disk encryption" and "Partitioned".	SafeGuard Easy "Boot Protection" encryption mode.

NOTE:
If you use external devices or expansion cards (sound cards etc.) please check if they support Microsoft power management and whether the computer can be set to hibernation mode, and returned from it, even if SafeGuard Easy is not installed.

20.4 Setting up hibernation

To achieve the best-possible security when activating hibernation mode, we recommend the following configuration:

1. In the Windows "Start" menu, select Settings/Control Panel/Power Options. In the *Hibernate* tab, select the "Enable hibernate support" check box.


Power Options Properties
Power Schemes
Advanced
Hibernate
UPS
When your computer hibernates, it stores whatever it has in memory on your hard disk and then shuts down. When your computer comes out of hibernation, it returns to its previous state.
Hibernate
Enable hibernate support.
Disk space for hibernation
Free disk space: 2,520 MB
Disk space required to hibernate: 255 MB

2. If two users are sharing one SafeGuard Easy computer, open the *Advanced* tab. In it, select the Options "Prompt for password when computer goes off standby and hibernate" field.

3. Now start SafeGuard Easy Administration.

4. Activate Pre-Boot Authentication (if you have not yet done so) in General/Password settings/Password at system start.

5. Encrypt the operating system partition via Encryption/Drives/Hard disk drive.

   To protect your system we recommend that you also encrypt all your data partitions along with the operating system partition.

21 Toggling floppy disk and device encryption

To provide a workstation with maximum protection, we recommend that you enable SafeGuard Easy floppy disk and device encryption. However, some situations require flexible handling of the encryption mechanism.

With SafeGuard Easy you can enable or disable the encryption of floppy disk and removable media drives for the duration of one logon and define your own keys for particular temporary time periods. The temporary settings are reset again after the logged-on Windows user logs off, and the current system default settings apply again.

The prerequisite for temporarily changing the encryption settings is that authentication has taken place using SafeGuard Easy user data during PBA, and encryption is enabled for floppy disks/removable media.

To avoid problems please read the tips for removable media drive encryption listed on 'Notes' carefully.

21.1 Necessary user rights

The prerequisite for switching encryption is that the user has appropriate SafeGuard Easy rights. You specify whether a user can switch encryption for floppy disk or removable media drives in the SafeGuard Easy User settings, in "Rights" (see 'User rights').

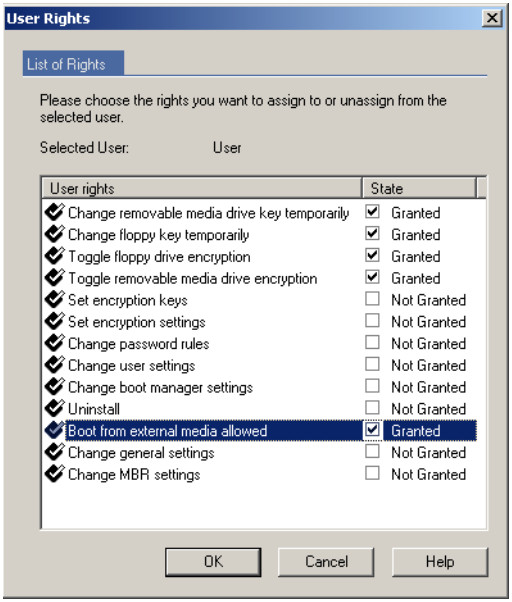
The following user rights are necessary:

- To switch encryption:

  - Toggle floppy drive encryption
  - Toggle removable media drive encryption

- To set a temporary key:

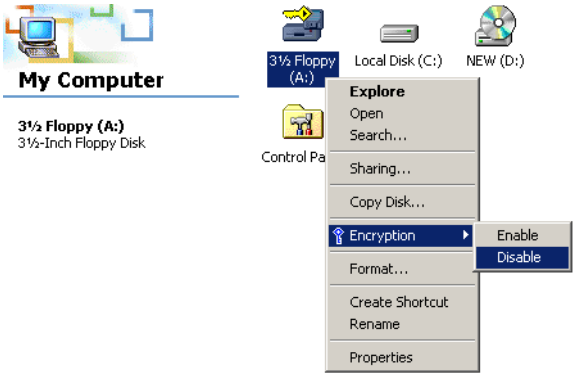
  - Change removable media drive key temporarily
  - Change floppy key temporarily



21.2 Switching encryption

You use Windows Explorer to switch the encryption status. For this purpose, SafeGuard Easy adds an extra menu item called "Encryption" to the Windows Explorer context menu.

If you click with the right-hand mouse button on an encrypted drive, you see a command for switching the encryption of a floppy disk or removable media drive on/off.



NOTE:
You can set the encryption status individually for each removable media drive!

21.3 Assigning keys with SgeCrypt

You use the SGECRYPT tool to assign new keys for the duration of one logon.

To run SGECRYPT, select Programs/Utimaco/SafeGuard Easy/**Switch floppy and device encryption**.

You can select from the following options:

- **Select key type**
  Specifies whether the key is to apply for floppy disks or removable media.

- **Use system key**
  Enabled (check box selected):
  The key set on the workstation (for example, during installation) for floppy disks or removable media drives will be used.

  Disabled (check box not selected):
  A new key will be used.

Before you can select a system key, it must also be set on the workstation. If this is not the case, a user with appropriate rights can later set this system key in Administration.

- **Temporary key**
  The temporary key only applies for the duration of one work session. When the computer restarts, it is deleted and the system key is enabled again.

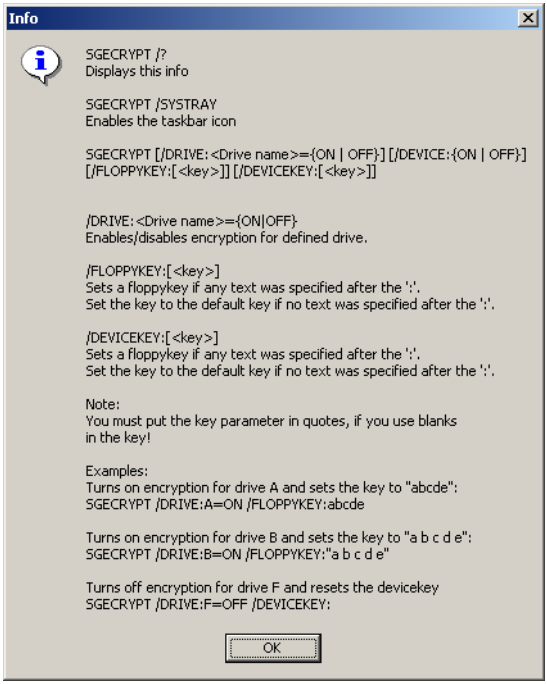
- **Show icon in taskbar**
  Displays an icon in the taskbar which the user can click to display this dialog. The setting only applies for the currently-logged on user. No Windows administrator rights are necessary to display/ not display the icon.

21.4 Using the command line to switch encryption settings

Floppy and device encryption can also be started from the command line.

Enter the following to display possible parameters:

```
SGECRYPT /?
```


Info
SGECRYPT /?
Displays this info
SGECRYPT /SYSTRAY
Enables the taskbar icon
SGECRYPT [/DRIVE:<Drive name>={ON | OFF}] [/DEVICE:{ON | OFF}]
[/FLOPPYKEY:[<key>]] [/DEVICEKEY:[<key>]]
/DRIVE:<Drive name>={ON|OFF}
Enables/disables encryption for defined drive.
/FLOPPYKEY:[<key>]
Sets a floppykey if any text was specified after the ':'.
Set the key to the default key if no text was specified after the ':'.
/DEVICEKEY:[<key>]
Sets a floppykey if any text was specified after the ':'.
Set the key to the default key if no text was specified after the ':'.
Note:
You must put the key parameter in quotes, if you use blanks
in the key!
Examples:
Turns on encryption for drive A and sets the key to "abcde":
SGECRYPT /DRIVE:A=ON /FLOPPYKEY:abcde
Turns on encryption for drive B and sets the key to "a b c d e":
SGECRYPT /DRIVE:B=ON /FLOPPYKEY:"a b c d e"
Turns off encryption for drive F and resets the devicekey
SGECRYPT /DRIVE:F=OFF /DEVICEKEY:
OK

21.5 Notes

- **Keys and algorithms**
  A removable media drive/floppy drive is encrypted by the key as well as the algorithm. You should find out which algorithms are being used for floppy and/or removable media drives at each workstation.

  Example: Floppies on your computer are encrypted with a DES algorithm. You store important data on a floppy disk so that you can access it again on another computer. If the floppy drive on this workstation is encrypted with IDEA, you will be unable to access the data on the floppy.

- **Reading encrypted media**
  You need to be careful if encrypted floppies/removable media are to be read in an unencrypted drive, and vice versa. If you insert an encrypted floppy/removable medium into an unencrypted drive, a system message will warn you that the file system on your floppy disk is incorrect. If you format the floppy disk because of this message, all files stored on it will be deleted. If a removable medium/floppy is accessed, but cannot be read, e.g. because encryption is active, a new message is displayed, warning you all files stored on the floppy disk will be deleted if you format it.

- **Switching encryption on/off**
  The right to switch the encryption of floppies and/or removable media drives on/off in SafeGuard Easy Administration is effective immediately, while the granting of new rights for SGECRYPT only takes effect after the machine is rebooted.

- **Warning message**
  If you access an unformatted or encrypted floppy disk/removable medium, the system displays a message warning you all files stored on the floppy disk will be deleted if you format it.

22 FIPS 140-2 (Level 1) certification

The FIPS certification describes security requirements for encryption modules. For example government bodies in the USA and in Canada require FIPS 140-2-certified software for particularly security-critical information.

The indicator that a SafeGuard Easy installation is FIPS-compliant is that only particular algorithms can be used for encryption. These are:

- AES-128
- AES-256
- 3DES

If SafeGuard Easy is installed in FIPS mode, an icon is displayed in the taskbar.

22.1 New functions

To meet the requirements involved in FIPS 140-2 certification, SafeGuard Easy now supports these two new types of functionality:

Known Answer Test (KAT)
The Known Answer test is performed to test whether the encryption algorithms used work correctly and supply correct results. The KAT is performed for all crypto-algorithms permitted by FIPS, including the hash function HMAC-256 which is used during the integrity check.

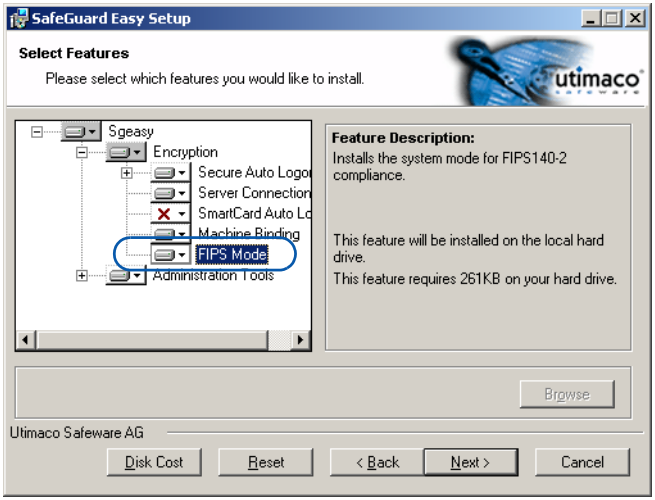
For the KAT (Known Answer Test), an encryption module encrypts a defined data block and checks the encryption result, if the generated encrypted data are the expected data. If the result is incorrect, the encryption module must block every other encryption process. The SafeGuard Easy encryption drivers automatically perform a Known Answer Test (KAT) after the driver has been initialized. The KAT is performed for encryption and decoding. The installed encryption modules within the SafeGuard Easy system core also perform the same tests.

Integrity check
An integrity check is performed for the encryption modules to ensure that the modules have not been changed. If an integrity check fails, the system stops all other processes. This test is performed for SafeGuard Easy's encryption driver files and the encryption modules within the SafeGuard Easy system core. In addition, the integrity check is performed for the system data within the system core, to show any illegal manipulations.

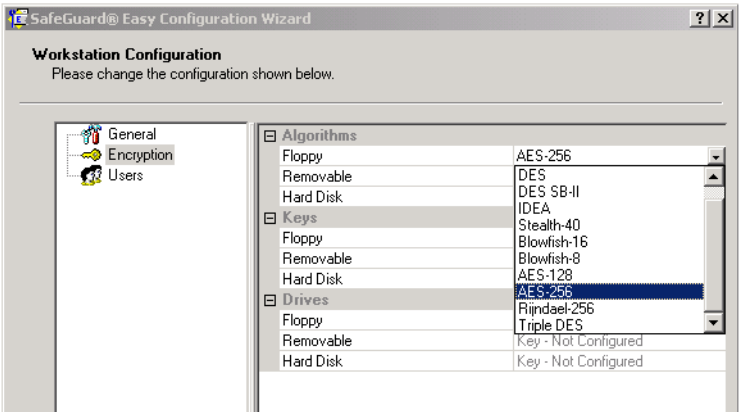
As soon as SafeGuard Easy has been installed to be FIPS-compliant, both test procedures are performed for the system kernel and Win32 mode. And the KAT (Known Answer Test) too, if FIPS mode is not active.

22.2 Installing SafeGuard Easy to be FIPS-compliant

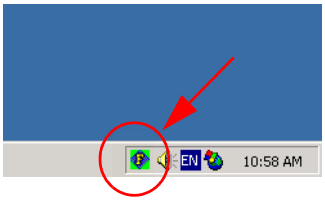
A setting during installation ("FIPS mode") specifies whether a SafeGuard Easy system should be FIPS-compliant.



Later on, during the installation, one of the required algorithms must be selected for each of the different disk drives (AES-128, AES-256, 3DES).



After the installation has finished, an icon in the System Bar shows that SafeGuard Easy is running in FIPS mode.



During the installation, if other algorithms than the permitted ones are selected, SafeGuard Easy displays an error message.

After the user confirms the error message SafeGuard Easy interrupts the installation and the user must restart it.

22.3 Secure use of SafeGuard Easy in certified configuration

To enable SafeGuard Easy to be implemented in a certified configuration, while also ensuring the maximum security provided with the product, the system should be configured as follows:

- Installation with PBA
- Minimum password length: 6 characters
- Use encryption algorithms AES-128, AES-256 or 3DES.
- Activate complete encryption of the hard disk
- Switch on floppy/removable media encryption
- Users cannot switch floppy/removable media encryption on or off
- Activate SafeGuard Easy's screen lock
- When defining keys manually, enter as large a number of randomly selected characters (max. 32 characters) as possible. No trivial keys should be assigned as they can be guessed easily by an attacker.

23 SafeGuard Easy and Lenovo ThinkVantage Technologies - Embedded Security Subsystem (Lenovo ESS Chip)

The Trusted Computing Group (TCG) (a union of international software and hardware manufacturers), was formed with the key objective of enhancing the security and authenticity of modern computer platforms and operating systems.

The basic technology behind this objective is the Trusted Platform Module (TPM): a cryptographic hardware chip on the motherboard, which serves as a secure key store, a cryptographic device, and a random number generator.

Similar to tokens, the TPM needs software applications to unleash its full power. In its basic form, the TPM can manage keys securely and can make these keys available for users and applications via standard mechanisms such as a Cryptographic Service Provider (CSP). The TPM as such does not encrypt any operating system or user data.

Beyond this, the use of the TPM enables completely new security concepts, such as the binding of a user to a specific machine.

Lenovo already equips a large number of their notebooks and desktop PCs with a TCG-compliant security chip. Lenovo calls the system ESS (Embedded Security Subsystem) and the associated client software "Client Security Software" (CSS). For some time Lenovo has been the leading manufacturer of notebooks with TPM and until quite recently was the only manufacturer in the market with an established solution.

Utimaco Safeware is the first professional security manufacturer to extend the Lenovo offering with an ESS-capable transparent hard disk encryption solution, along with other ESS-enabled security products. This pairing allows users to benefit from hardware-based security, while maintaining full control over their IT infrastructure.

For more information about TPM, ESS and CSS please refer to your Lenovo documentation.

23.1 SafeGuard Easy and TPM

SafeGuard Easy TPM support provides extended functionality for PCs with an ESS/TPM chip. The most important functions are:

- **Client Security Solution Integration (CSS)**
  SafeGuard Easy has a specially-designed function that allows users of workstations with a TPM chip to continue using CSS. If SafeGuard Easy is combined with CSS it gives users the option of automatically logging on to TPM immediately after Pre-Boot Authentication. In this situation the data is saved by SafeGuard Easy and automatically transferred to the SafeGuard Logon process. This means that the user does not have to remember yet another password.

- **Generate a random key using TPM**
  The Lenovo ESS/TPM chip has a generator that generates random numbers. SafeGuard Easy uses this mechanism to generate session keys and random keys.

- **Save the connection between SafeGuard Easy Client and SafeGuard Easy Server using TPM**
  SafeGuard Easy can also use the TPM generator to back up the client/server connection as part of its central administration tasks. Within the framework of their central administration tasks, SafeGuard Easy Client and SafeGuard Easy Server each generate one RSA key pair to mutually authenticate themselves and to secure the connection to the database. This key pair can also be generated by the ESS/TPM chip.

- **Machine binding**
  This is used to bind a hard disk to one specific ESS/TPM. If this hard disk is then stolen, it can no longer be used in any other computer, even if the password is known.

23.2 Preparing the ESS/TPM Chip for use

Before the chip can be used (and **before installing SafeGuard Easy**), you should make the following preparations:

1. Ensure that the ESS chip is activated in the BIOS.

2. Install the Atmel driver for the ESS/TPM chip.

   Not required with CSS >=6.0.

3. Install the SMBUS driver (each Lenovo ThinkPad has its own driver).

4. For SafeGuard Easy, you need these versions of Lenovo "Client Security Software" (CSS).

   - **To generate random keys and CSS integration:**
     "Client Security Software" (CSS) version 5.21 and higher
   - **For client/server authentication:**
     "Client Security Software" (CSS) version 5.30 and higher

23.3 Required settings for CSS integration

To integrate SafeGuard Easy in CSS you must first configure CSS in the appropriate way. For more information, please refer to the CSS manual.

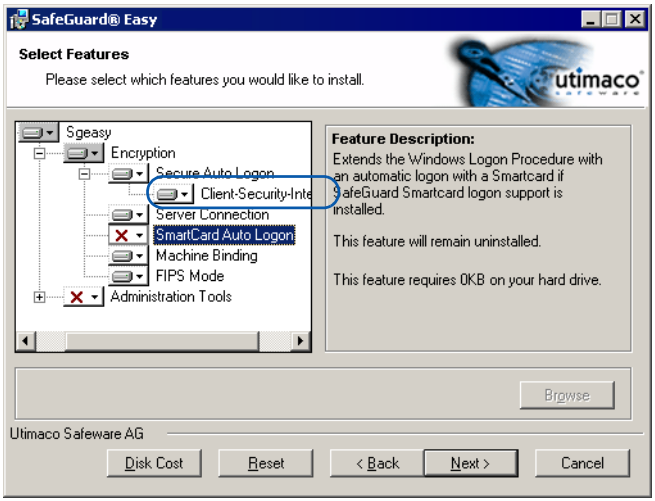
To combine CSS and SafeGuard Easy:

1. Prepare the chip for use.

2. When you configure the Client Security Software (CSS) you must ensure that "Replace the normal Windows logon with the saved Lenovo security client logon" is active!!!

   Not required with CSS >=6.0.

3. Install SafeGuard Easy.
   When you install SafeGuard Easy you must ensure that the "Client Security Integration" option is active.



Apart from this, no other special configuration settings are required in SafeGuard Easy.

4. After the PC restarts you will see a different logon screen which prompts you to enter a "Passphrase" instead of the Windows password.

CSS integration and SafeGuard Easy's Secure Automatic Logon (SAL) function

Once the Windows data has been entered, the SAL places it in a protected area and loads it again, whenever the user successfully logs on in PBA, to automatically log them on to the operating system ('Configuring Windows logon').

A similar thing happens when CSS integration and SAL are used together on one PC. The passphrase is encrypted and stored so that the user does not need to enter it again. The user will then only be prompted to enter logon data during PBA.

NOTE:
If SAL was active during the normal Windows logon, you must delete the `SGSAL.dat` file (which is stored in <system drive>`/System32`) before integrating CSS.

`SGSAL.dat` must be reloaded because TPM data is stored in a different format from normal Windows logon data. For this reason, no `SGSAL.dat` file should be present if you want to use CSS/SAL.

23.4 Required settings for generating random keys using TPM Chip

To generate random keys using the ESS/TPM chip you must make a number of registration entries **before installing SafeGuard Easy**.

To generate a random key with the TPM chip:

1. Prepare the chip for use (see 'Preparing the ESS/TPM Chip for use').

2. In the Windows Registry under

   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   SGEasy

   enter new subkeys:

   Cryptographic Service Provider [STRING]

   a) with CSS<= 5.40 enter:
   "IBM Embedded Security Subsystem Enhanced CSP"
   b) with CSS>= 6.0 enter
   "ThinkVantage Client Security Solution CSP"

   UseCSPRandomGenerator [DWORD]
   Set the value to "1".

3. Install SafeGuard Easy.

No other configuration settings are required and the ESS/TPM chip will now generate the random key.

23.5 Required settings for using the TPM chip to secure the Client/ Server Authentication

Settings for Client Security Software <= 5.40

The chip's administrator password safeguards the generation of key pairs via the ESS/TPM chip. The administrator password is defined during the installation of the CSS software. If SafeGuard Easy is distributed to several Clients with a TPM chip as part of a central installation, the Client users will be prompted to enter the administrator password in a dialog.

In networks with several TPM clients, normal users do not usually know the chip's administrator password. It is also often the case that administrators would like to use the same password for all TPM computers in the network.

For this purpose, SafeGuard Easy includes a proprietary tool with which you can generate an encrypted file using the chip's own administrator password. This file can then be distributed to TPM clients as part of a central installation. SafeGuard Easy then automatically fills in the dialog on the client side which prompts for the administrator password. As a result, the RSA key is generated without any user interaction.

To generate RSA key pairs using the TPM chip:

1. Prepare the chip for use in a client/server configuration (see 'Preparing the ESS/TPM Chip for use').

2. In the Windows Registry on the client/server, under:
   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   SGEasy
   enter new values:

   Cryptographic Service Provider [STRING]
   "IBM Embedded Security Subsystem Enhanced CSP"

   ForceCSPUsage [DWORD]
   Set the value to "1".
   (ForceCSPUsage also generates the random keys.)

3. On a PC where SafeGuard Easy is installed, run the `SGTpmApn.exe` tool and create the encrypted file using the administrator password for the ESS/TPM chip. The default file name is `SGTPMGNA.DAT`

   If you want to rename this file, enter the following in the client's Windows Registry in

   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   SGEasy

   ESSAdminPassword [STRING]
   You must enter the file with the administrator password as the value, (e.g.: `D:\Programs\Utimaco\SafeGuard Easy\AdminPW.dat`)

4. Distribute encrypted files together with SafeGuard Easy packets to clients. The file with the administrator password must be present in the SafeGuard Easy installation directory.

Immediately before the RSA key is generated, SafeGuard Easy starts a monitor which reads the administrator password from this file, automatically fills the ESS CSP password dialog and then deletes the file.

After SafeGuard Easy has been installed, the RSA key pair is generated automatically and the user does not need to make any further configuration settings.

Settings for Client Security Software >= 6.0

From CSS Version 6.0 the chip's administrator password is not required, and the RSA key pair is generated interactively. As a result, there is no need to create and deploy a encrypted file with the supplied SafeGuard Easy tool, as was the case with CSS <= 5.40.

To generate RSA key pairs using the TPM chip:

1. Prepare the chip for use in a client/server configuration (see 'Preparing the ESS/TPM Chip for use').

2. In the Windows Registry on the client/server, under:
   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   SGEasy
   enter new values:

   Cryptographic Service Provider [STRING]
   "ThinkVantage Client Security Solution CSP"

   ForceCSPUsage [DWORD]
   Set the value to "1".
   (ForceCSPUsage also generates the random keys.)

NOTE:
Generating key pairs using a TPM chip is much slower than a purely software solution. This may have an impact on response times. The impact on response times is only cause by the client/server authentication, not by encryption processes.

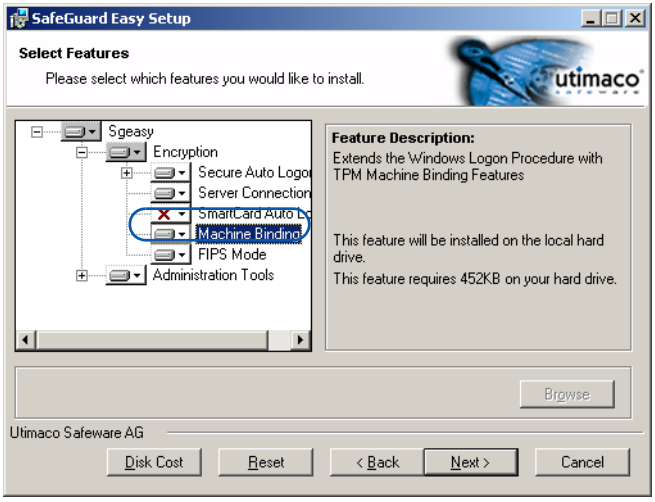
23.6 Required settings for Machine Binding

The Machine Binding establishes a unique connection between the machine and its hard disk. This is achieved through a signature that is checked against the reference signature created during the initial machine binding. This reference signature is then stored in the registry. The boot process will only proceed if both signatures are identical. In any other case, the boot process is terminated.

To combine Machine Binding and SafeGuard Easy:

1. Prepare the chip for use.

2. Install SafeGuard Easy.
   When you install SafeGuard Easy you must ensure that the "Machine Binding" option is active.



   Apart from this, no other special configuration settings are required in SafeGuard Easy.

23.6.1 Initial Machine Binding

When the system is started up for the first time after the machine binding feature has been installed, the *SafeGuard Authentication Machine Binding Wizard* is launched, informing the user that the machine binding has not yet been activated.

SafeGuard Authentication - Machine Binding
[SafeGuard® Authentication]
utimaco
Welcome to the SafeGuard Authentication Machine Binding Wizard!
SafeGuard Authentication protects your hard-disk by providing secure authentication and also ensures that your hard-disk cannot be used in any other pc or laptop but the current one.
The machine binding for this computer has not yet been activated. To activate it, type in the administrator passphrase for your computer's hardware security chip. Once the password has been confirmed, a secret key will be generated for your computer.
Press Continue to start the process, or Shut down to quit.
Continue >>
Shut down

NOTE:

CSS < 6.0: Security Chip password is required.

CSS >= 6.0: Security Chip password is NOT required.

Click **Continue** to start the initial machine binding process.

Since any private key operation with the security chip requires a password, the Security Chip password must be entered.

CSS>=6.0 does not require a Security Chip password.

Enter Administrator Password
Before you can complete an IP Security certificate request, you must enter the IBM Security Chip password below.
Too many consecutive incorrect entries will cause the security subsystem to be locked for increasing periods of time.
OK
Exit

A dialog confirms a successful machine binding. The local hard drive can now only be used with the current computer.

SafeGuard Authentication - Machine Binding Complete
[SafeGuard® Authentication]
utimaco
Congratulations! The machine binding process has finished successfully.
SafeGuard Authentication is now bound to your computer's hardware. Your local hard drive can now only be used to start-up this computer.
Please refer to your user manual for backup and recovery procedures.
Close

With each subsequent boot the software will check the status of the machine binding and will proceed only if both signatures are identical.

23.6.2 Machine Binding failed

SafeGuard Authentication - Machine Binding Failed
[SafeGuard® Authentication]
utimaco
The machine binding verification has failed!
This can happen if either the local hard drive is used in a different computer as it has been registered for, or if the configuration of the local security hardware has changed or been corrupted.
Please contact your IT security administrator for additional support.
Shut Down
Recovery

There are several situations that can cause the signature verification to fail:

- The hardware security module is deactivated.
- The hardware security module is damaged.
- The hardware security module's master key has changed.
- The reference signature is corrupted.
- The reference signature is missing.
- The key pair used for the signing operation is corrupted.
- The CSP used is corrupted.
- The CSS configuration was changed.

To get access to the system when the machine binding failed, this dialog provides a recovery functionality.

To restore the system using a backup of the Embedded Security System (ESS) please refer to your Lenovo documentation.

23.6.3 Machine Binding recovery

To get access to the machine when machine binding failed, click the **Recovery** button.

In this dialog the Security Chip Password which was used for the initial machine binding needs to be presented. It also needs to be presented when the password has been changed after the initial machine binding. If Recovery is used, because the old chip has been replaced by a new Security Chip, the password for the old chip also needs to be used for recovery.

Starting CSS version >= 6.0 this dialog is replaced by the default „SafeGuard Authentication - Recovery“ dialog, which asks for Windows user name, password and domain.

After you have gained access to the machine, you must perform the initial machine binding again, if the verification failed for the following reasons:

- The hardware security module is damaged.
- The hardware security module's master key has changed.
- The reference signature is corrupted.
- The reference signature is missing.
- The key pair used for the signing operation is corrupted.

Before performing machine binding is done, you must

1. delete the following values in the Windows registry:

   - **Machine Binding**
   - **Recovery**

     under this key:

     HKEY_LOCAL_MACHINE
     SOFTWARE
     Utimaco
     SGLogon
     Embedded Security System

IMPORTANT:

These values have to be deleted before the machine binding is done again. If these values are present during the machine binding process, there may be situations in which you can no longer access the system,

2. You have to set back the data stored on the Security Chip using Lenovo tools.

The initial machine binding process starts automatically at the next system startup.

23.6.4 Recovery mode configuration

Beside the described default dialog for system recovery, the SafeGuard Authentication TPM Support includes a second dialog in which you can authorize the recovery process. In this dialog you must enter the user name and password (optional domain name) of a user with administrative privileges to gain access to the system.

You can specify which dialog is to be used via an ADM template which is installed when TPM support is enabled. This setting can be found in the Management Console under:

Computer Configuration
\Administrative Templates
 \SafeGuard
  \Authentication
   \Machine Binding
    \Recovery

You can select *Recovery Type*

- **Administrative Account**
  to specify that the Windows user name and associated password are to be used, or
- **TPM Password (default)**
  to specify that the Security Chip passphrase is to be used,

as appropriate.

Enter the user name and password of a user that has an account on this machine. The domain name is optional.

NOTE:
This user must have administrative privileges on this machine.

24 SafeGuard Easy and Lenovo ThinkVantage Technologies - Rescue and Recovery

SafeGuard Easy supports Lenovo's efficient Rescue and Recovery backup and recovery function, so users can use this method along with operating system partitions encrypted with SafeGuard Easy: when combined with hibernation support, they provide functionality that is unique amongst disk encryption products!

24.1 Overview

The main function of Lenovo's Rescue and Recovery™ is to restore data at the press of a key. Even if the primary operating system is damaged and no longer boots, Rescue and Recovery™ saves data via an emergency environment. You can access the rescue tools from the Microsoft Windows Desktop or by pressing the blue "ThinkVantage" (formerly Access IBM) key integrated in Lenovo systems. However, Rescue and Recovery™ also supports non-Lenovo systems.

Lenovo's Rescue and Recovery is most useful for mobile users who do not have access to an administrator when they are on the road: they can use it to restore their system themselves.

Utimaco Safeware is currently the only vendor of hard disk encryption tools to offer users of Lenovo PCs and notebooks a way to restore an encrypted system without losing encryption. This solution protects all the data on the system and maintains the security of the data.

For more information on Lenovo's Rescue and Recovery™ please refer to the relevant Lenovo documentation.

24.2 Rescue and Recovery with SafeGuard Easy

SafeGuard Easy is integrated with Rescue and Recovery functionality and supports the Lenovo features such as the "ThinkVantage“ (Access IBM) blue button on the keyboard of Lenovo notebooks or the blue "Enter" button on PC keyboards.

After encryption is completed, the user is prompted to create a new backup containing the new changes made. To allow this, the system contains, for example, the SafeGuard Easy driver, which is used to restore this backup. (Below, a secure backup with SafeGuard Easy and its drivers is referred to as an "SGE backup").

SafeGuard Easy is unaffected by a system restore and all the encryption settings are still in place so there is no need to reinstall any software. The user can get back to work straight away and does not need to restart encryption.

24.2.1 Advantages of combining Rescue and Recovery™ and SafeGuard Easy

- SafeGuard Easy encrypts the entire hard disk drive including temporary files, the paging file, hibernation and memory dump file, and protects them from unauthorized access by prompting for the SafeGuard Easy user data at logon.
- All Rescue and Recovery backups are encrypted provided they are stored on an encrypted local hard disk drive.
- Rescue and Recovery restores a damaged system without the need to re-install SafeGuard Easy and encrypt the hard disk drive once again.
- You can only restore a backup with SafeGuard Easy in Rescue and Recovery environment if SafeGuard Easy user data has already been entered at Pre-Boot Authentication.

24.2.2 Requirements

- Lenovo PC/notebook
- Latest BIOS for the PC/notebook
- Supported Rescue and Recovery™ versions:
  - Rescue and Recovery™ 1.0 (Build 033)
  - Rescue and Recovery™ 2.0 (Build 2.00.0170)
  - Rescue and Recovery™ 3.0 (Build 3.00.0029.00)
  - Rescue and Recovery™ 4.0 (Build 4.0.0114)
  - Rescue and Recovery™ 4.2 (Build 4.20.0510)

24.3 Installation

In the installation examples below it is assumed that the Rescue and Recovery environment is not installed in the service partition. You will find details of how to manage the service partition in a separate chapter.

When Rescue and Recovery software is installed on a hard disk without a service partition the following default settings apply for it:

- The Rescue and Recovery environment is installed on a virtual partition on the workstation's hard disk C: partition (primary partition of the master hard disk).
- The virtual partition contains the two folders \minint and \preboot. These two folders are protected by Rescue and Recovery.
- By default the backups are saved in the C:\RRUbackups folder. This folder is protected by Rescue and Recovery if it is stored on a local partition on the primary hard disk drive. If so, it cannot be deleted or removed.

Please note the sequence in which Rescue and Recovery and SafeGuard Easy are installed in the next few sections.

24.3.1 When neither Rescue and Recovery nor SafeGuard Easy are installed

1. Uninstall any version of Rescue and Recovery with Rapid Restore older than 4.0.

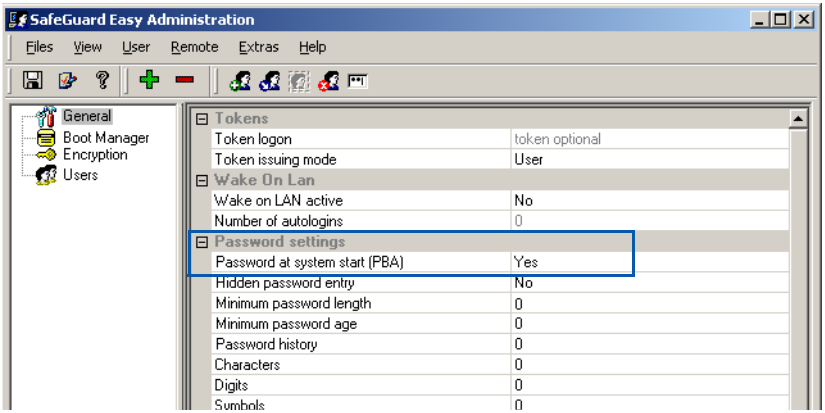
2. Install Rescue and Recovery.

3. Install SafeGuard Easy, version 4.10 onwards.

   SafeGuard Easy checks if the correct version of Rescue and Recovery is installed and adds its own files and configurations to the Lenovo recovery environment.

   Check that Pre-Boot Authentication is activated, so no unauthorized backups can be restored.

   You activate Pre-Boot Authentication when installing SafeGuard Easy, or later in SafeGuard Easy Administration via General/Password Settings/Password at system start.



24.3.2 SafeGuard Easy is already installed

SafeGuard Easy, version 4.10 onwards is installed

1. Install Rescue and Recovery

2. Before the reboot, start the tools from the SafeGuard Easy folder
   - MBRsync.exe
   - WinPERepair.exe

Versions of SafeGuard Easy older than 4.10 are installed

1. Update SafeGuard Easy to version 4.10 or higher

2. Install Rescue and Recovery.

3. Before the reboot, start the tools from the SafeGuard Easy folder
   - MBRsync.exe
   - WinPERepair.exe

or

1. Install Rescue and Recovery

2. Before the reboot, start the tools from the SafeGuard Easy folder
   - MBRsync.exe

3. Update SafeGuard Easy to version 4.10 or higher.

WARNING:
If Rescue and Recovery is installed after SafeGuard Easy, ensure you run the "MBRsync.exe" and "WinPERepair.exe" tools before the reboot that activates Rescue and Recovery. If they are not started you see the error message "Error! Reference source not found". The tools are located in the SafeGuard Easy folder: double-click them to start them.

24.4 Upgrade

Upgrade implies that SafeGuard Easy from version 4.10 onwards and Rescue and Recovery™ are installed and you want to upgrade one to a newer version.

24.4.1 Upgrading SafeGuard Easy

If you upgrade SafeGuard Easy, this updates the entire system, so you will not need to set any further configurations.

24.4.2 Upgrading Rescue and Recovery

If you upgrade Rescue and Recovery, run the MBRsync.exe and WinPERepair.exe tools before you reboot after the update. The tools are located in the SafeGuard Easy folder: double-click them to start them.

24.5 Uninstallation

You must take certain factors into account before you can uninstall the software products.

- We recommend that you uninstall Safeguard Easy first, and then Rescue and Recovery.
- If you uninstall Rescue and Recovery before SafeGuard Easy, you must run the MBRsync.exe tool before rebooting.
- Do not uninstall SafeGuard Easy immediately after the system has been restored. After a system restore, boot the PC once and then uninstall SafeGuard Easy.

24.6 How to create a backup

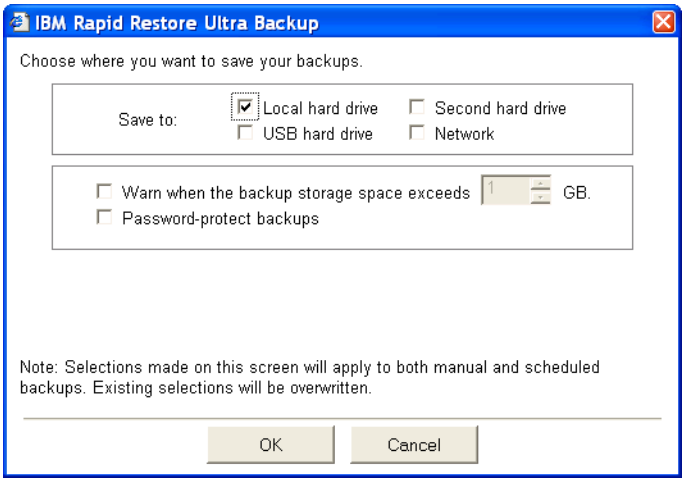
General note:
The screenshots in the sections that follow show extracts from version 4.0 of Rescue and Recovery™ (Build 033). The user interface features may vary in later versions, but the described functionality is identical.

You create backups using Rescue and Recovery™ software in Windows. On PCs on which Rescue and Recovery™ is already installed, and then SafeGuard Easy, a message appears prompting the user to create a new backup of the system.

Before you create a backup of your system using Rescue and Recovery, please read the documentation provided by Lenovo.

SafeGuard Easy only provides support for saving the backups:

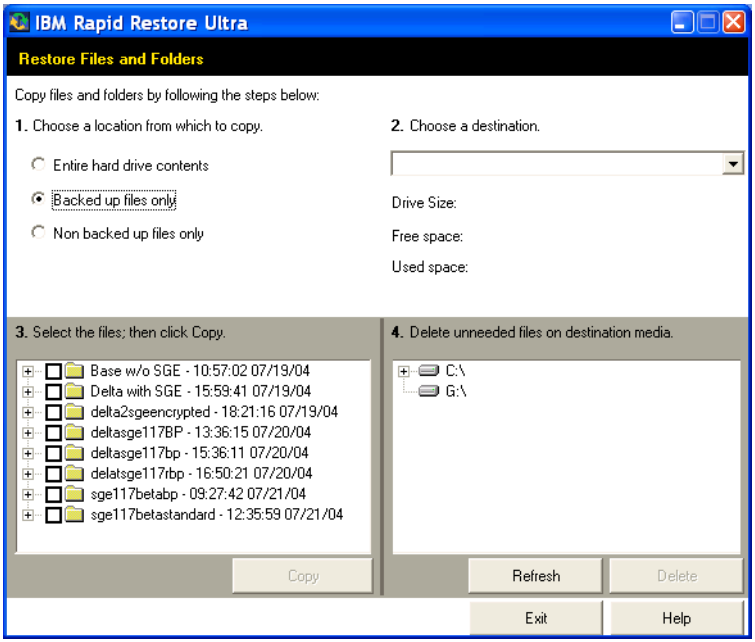
- to the local hard disk
- second hard disk
- USB hard disk
- network
- USB memory stick
- CD/DVD


IBM Rapid Restore Ultra Backup
Choose where you want to save your backups.
Save to:
Local hard drive
Second hard drive
USB hard drive
Network
Warn when the backup storage space exceeds
1
GB.
Password-protect backups
Note: Selections made on this screen will apply to both manual and scheduled backups. Existing selections will be overwritten.
OK
Cancel

By default the backups are saved in the C:\RRUbackups folder. This folder is protected by Rescue and Recovery if it is stored on a local partition on the primary hard disk drive. If so, it cannot be deleted or removed.

24.7 Restoring file backups

Rescue and Recovery™ can restore files or folders from backups which in which SafeGuard Easy is installed. The user simply has to start Windows, and then the Rescue and Recovery™ Software, and restore the selected files. The user does not need to reboot their machine after the restore is completed: they can work with their files immediately.



24.8 Restoring the system

To restore a system backup which includes SafeGuard Easy, the user must boot into the Rescue and Recovery environment. To do so, press the blue "ThinkVantage“ (Access IBM) button on the Lenovo notebook keyboard or the blue "Enter" button on the PC keyboard.

Note concerning Rescue and Recovery™ 2.0:
We generally recommend that you recover the entire hard disk when you perform a restore.

However, if you accidentally select the "Recover only the Windows-operating system and applications from a backup" option, Utimaco does not guarantee that the SafeGuard Easy files will be completely restored. However, if there are problems with booting, do not worry about negative consequences for your system. When you restart it, simply press the Lenovo keys on your PC or notebook to access the Rescue and Recovery™ environment and recover your entire hard disk again.

24.8.1 Boot environment

To boot into the Rescue and Recovery environment, certain prerequisites must be met.

SafeGuard Easy **allows** the user to boot into the Rescue and Recovery environment …

- *From the local hard disk*
  The virtual partition on the local hard disk or the local service partition

SafeGuard Easy **does not allow** the user to boot into the Rescue and Recovery environment.

- *From a bootable CD*
- *From a bootable USB hard disk*

If the Rescue and Recovery is booted from an external device, SafeGuard Easy will be removed during the restore process.

To secure the system again you must reinstall SafeGuard Easy.

24.8.2 Restoring a SafeGuard Easy system

1. Start the Rescue and Recovery environment by pressing the blue "ThinkVantage“ button on the Lenovo notebook keyboard or the blue "Enter" button on the PC keyboard.

2. The system displays the Pre-Boot Authentication prompt in which the user enters their SafeGuard Easy logon details (credentials).

3. The system displays the user interface for Rescue and Recovery.

4. The welcome screen appears. Click the Next button to continue.

5. In the menu on the left-hand side, select the Restore Backup option.

6. The system displays a dialog in which you can select the backup.

7. Select the backup and restore it.

24.9 Service and factory recovery partitions

Lenovo supplies new PCs with special pre-installed partitions. Lenovo calls these partition “service partition“ and “factory recovery partition“:

- Service partition: contains the Rescue and Recovery Boot environment.
- Factory recovery partition: contains all information for recovering the workstation’s factory settings.

If there is no service partition on the workstation, but you would like to create one, do so before installing SafeGuard Easy.

Please refer to the Lenovo documentation on how to create a service partition.

24.9.1 Features

The service and factory recovery partition have the following special features.

Operating System	SafeGuard Easy's Encryption Mode	Status of the two special partitions
Windows 2000	Partitioned	The partitions are not encrypted. Benefit: the Lenovo factory settings can be restored from the local hard disk. Disadvantage: hackers could access the unencrypted service partition and modify it.
Windows XP	Partitioned, Full disk encryption, Boot protection	
Windows 2000	Full disk encryption Boot Protection	The partitions are encrypted. Benefit: the entire boot environment is encrypted and can only be accessed when the SafeGuard Easy password is known. Disadvantage: the Lenovo factory settings cannot be restored from the local hard disk. If you want to restore the Lenovo factory settings you can do so by requesting a CD or DVD from Lenovo. Alternatively you can decrypt the hard disk via the emergency boot floppy disk, using the Sgeasy.exe tool which runs in DOS and uninstalls SafeGuard Easy.

We recommend that you encrypt the service partition or install Rescue Recovery environment on a virtual partition. The virtual partition is always secured as long as the Windows hard disk is encrypted.

24.10 What should I do, if ...

...if you reboot the machine and the system displays a SafeGuard Easy screen with a virus warning?

This screen may appear for the following reasons:

1. *There is a virus on your system.*

   Please contact your system administrator as soon as possible.

2. *The user installed, modified or uninstalled Rescue and Recovery system but forgot to run the MBRsync.exe command.*

   SafeGuard Easy detects changes made to the MBR and displays the virus warning if there are any. If you are sure that the message is caused by Rescue and Recovery, select the "Keep changes" menu option.

...if the operating system is damaged?
In this case you can restore your previously-saved backup (including SafeGuard Easy) using Rescue and Recovery.

Alternatively you can decrypt the hard disk via the emergency boot floppy disk, using the Sgeasy.exe tool which runs in DOS and uninstalls SafeGuard Easy. The hard disk is now in plain (unencrypted) text, and you can use rescue tools on it. If you (or any other user) do not have the right to uninstall SafeGuard Easy you can use the SafeGuard Easy Challenge Response Code Wizard to obtain the temporary right to uninstall SafeGuard Easy.

...if the hard disk is physically damaged?
If the hard disk is physically damaged, and it is not possible to decrypt it using the DOS Sgeasy.exe tool, contact Utimaco: we will put you in touch with one of our partners who specializes in rescuing physically damaged hard disks.

...if the SafeGuard Easy system kernel is damaged?
An overwritten MBR can be repaired with Sgeasy.exe or a previously-saved kernel can be restored to act as the system kernel.

...if the initial encryption has been interrupted and the computer cannot be booted up to Windows any more?
In this case contact Utimaco's support.

...if the final decryption has been interrupted and the computer cannot be booted up to Windows any more?
In this case contact Utimaco's support.

25 Compatibility with Absolute Computrace software

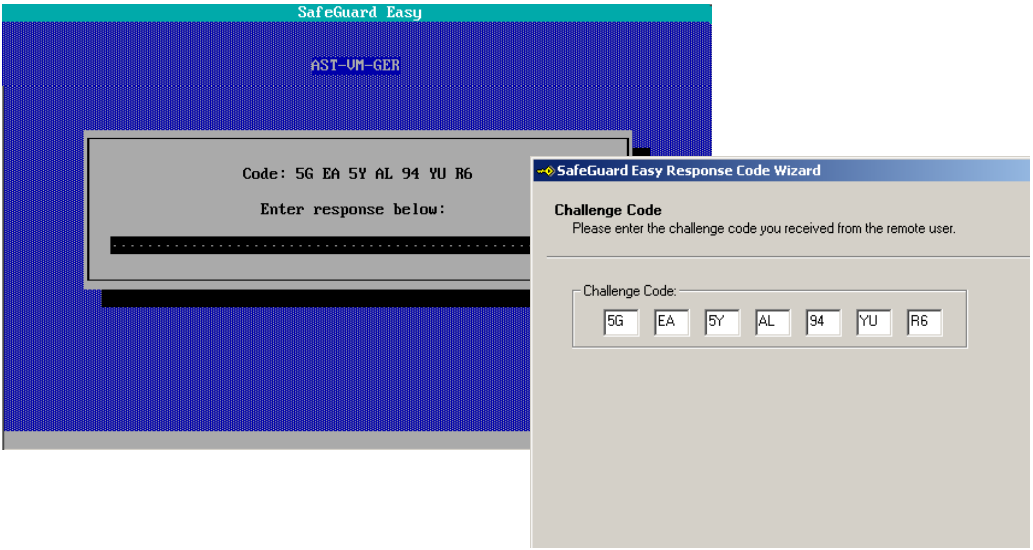
Lenovo now protects its new ThinkPad notebooks with many security features, including SafeGuard Easy and SafeGuard PrivateDisk, and so guarantees its users with high levels of mobile security. Alongside these products from the SafeGuard family, Computrace, from Absolute Software Corp. is also preinstalled on Lenovo notebooks.

If a notebook is stolen, Computrace helps trace it, as soon as it connects to the Internet, and the authorized user can also force confidential data to be deleted on the stolen notebook, if required. Computrace is the only provider whose software Lenovo integrates in the PC hardware (BIOS persistent agent).

As Computrace software is compatible with SafeGuard Easy it works with encrypted hard disks.

SafeGuard Easy is prepared for being compatible with Computrace. Full compatibility requires a Computrace software version which has not yet been released by Absolute Software (12/2008).

26 Remote maintenance (Challenge/Response)

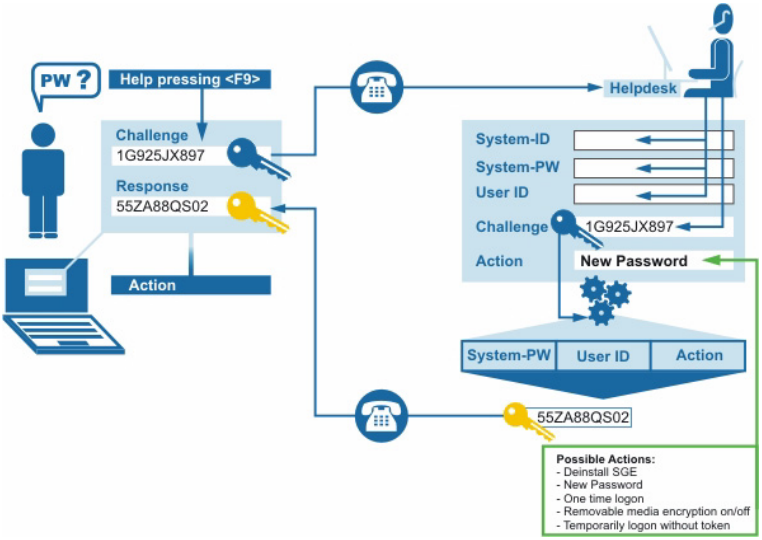


SafeGuard Easy includes a Challenge/Response procedure for resetting "forgotten" SafeGuard Easy or token passwords.

Challenge/Response is very secure and efficient:

- No confidential data is exchanged.
- Attempts to "eavesdrop" or use data gathered by "listening in" fail.
- Can also be used for devices without a network connection.
- The user can start working again after only a short interruption.

26.1 How it works



If a user (remote user) requires help, they must generate a challenge code in PBA. This challenge code is displayed as an ASCII character string on the remote user's screen. The user then calls their helpdesk and tells the helpdesk their user information and the challenge code. The helpdesk staff member runs the SafeGuard Easy Response Code Wizard, and generates a response code. The helpdesk staff then tell the user the response code by telephone or SMS. When the user enters this response code on the user PC, the user can reset their password.

Usually the following special rights can be assigned via Challenge/ Response:

- Setting a new user password (if the old has been forgotten)
- Uninstall SafeGuard Easy
- One-time logon (for example, for maintenance tasks)
- Temporarily grant right to switch floppy and device encryption (for the duration of one logon)
- Logon without required token for X logons
- Grant permission to issue a token

The Response Code Wizard can be installed either on a PC or on a helpdesk team member's PDA.

26.1.1 Installing PDA version of the Response Code Wizard

You will find the PDA version of the Response Code Wizard on the SafeGuard Easy CD.

1. Copy the `SGE_CRW.PPC30_ARM.cab` file from the \TOOLS folder on the SafeGuard Easy CD onto the PDA.

2. Access `SGE_CRW.PPC30_ARM.cab` using the PDA File Explorer. The installation is performed immediately.

3. After installation you must perform a soft reset.

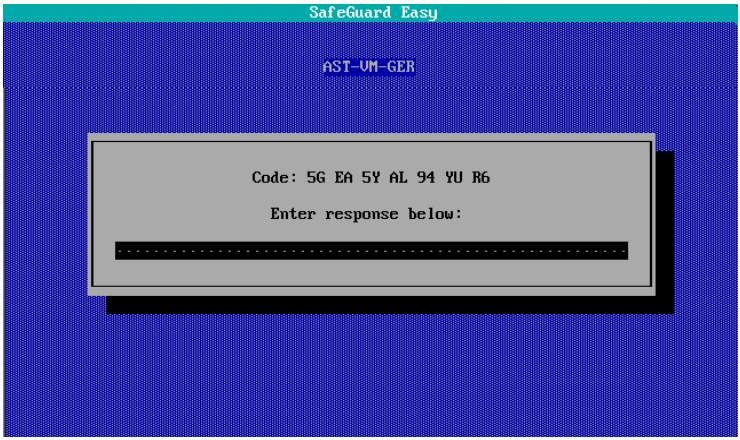
SafeGuard PDA must be installed on the PDA.

26.2 Generating a challenge code

The challenge code is generated by a user, for example if they have forgotten their SafeGuard Easy password. The challenge code can be generated in various ways, depending on the way the system was started:

System start with PBA

In the case of a **system start with PBA**, the user must enter their SafeGuard Easy user name during PBA and then go to the password field. After they press [F9] they see the challenge code.



System start without PBA

In the case of a **system start without PBA**, a floppy disk icon is displayed in the top left-hand corner of the screen, when the computer is booting. During this time period the user presses [F2]. The system displays the PBA logon dialog, and the user enters their SafeGuard Easy user name for PBA. They then move into the password field. After they press [F9] they see the challenge code.

Special case: Uninstallation

To uninstall SafeGuard Easy using Challenge/Response, you must use the uninstallation dialog to generate the challenge code (Start/Settings/Control Panel/Add/Remove Software and then the entry "SafeGuard Easy"). You cannot initiate uninstallation of SafeGuard Easy with via the Challenge/Response procedure **during PBA**.

26.3 Response Code

The administrator or helpdesk staff use the Response Code Wizard to generate the response code.

The person who generates the response code must know the data of a SafeGuard Easy user profile on the remote PC, for example the data user "Helpdesk". The user "Helpdesk" must have at least the same rights as the SafeGuard Easy user which is asking for help.

To let the user profile "Helpdesk" give special rights to the remote SafeGuard Easy user, the following additional user rights are required:

Planned Remote Command	Required SafeGuard Easy user right
Uninstall	Uninstall SafeGuard Easy
Set new user password	Change user settings
One-time logon	Change user settings
Temporarily grant right to switch floppy and device encryption	Switch floppy drive encryption
Logon without required token for X logons	Change user settings
Grant Permission to issue a token	---

26.3.1 Creating a response code

NOTE:
Requirement for generating a Response Code on a PC:
1) Response Code Wizard.

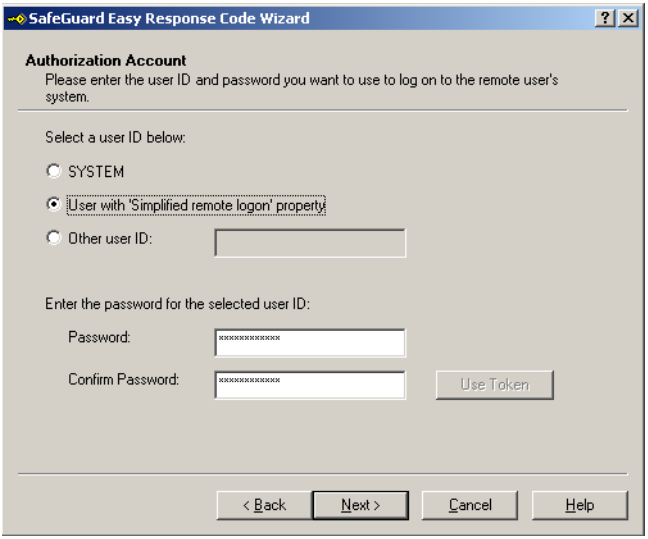
Requirement for generating a Response Code on a PDA:
1) SafeGuard PDA.
2) PDA Version of the Response Code Wizard.

To run the wizard, select **Programs/SafeGuard Easy/Utimaco/ Response Code Wizard**.

The first dialog displays information about the wizard. In the wizard, click [Next] to confirm that all entries are correct.

Authorization Account

In the “Authorization Account” dialog, select the SafeGuard Easy user with which you want to log on to the remote user’s system.


SafeGuard Easy Response Code Wizard
Authorization Account
Please enter the user ID and password you want to use to log on to the remote user's system.
Select a user ID below:
SYSTEM
User with 'Simplified remote logon' property
Other user ID:
Enter the password for the selected user ID:
Password:
Confirm Password:
Use Token
< Back
Next >
Cancel
Help

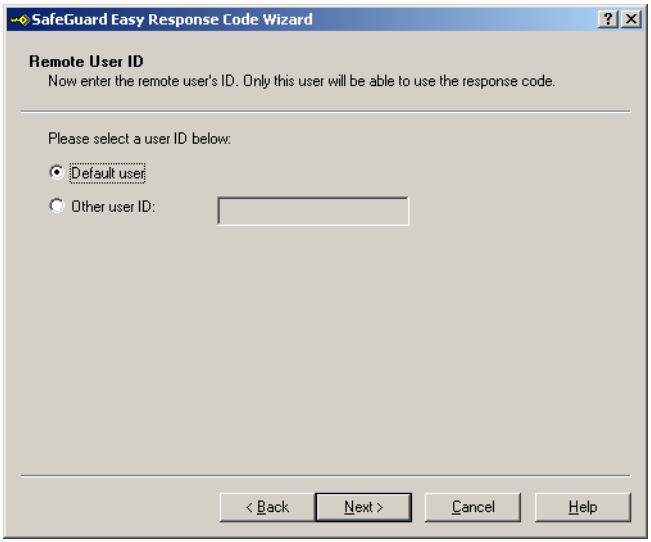
- **SYSTEM:**
  User name of the system administrator for SafeGuard Easy.
- **User with "Issue abbreviated C/R Code" property:**
  User to whom this property has been assigned on the target system. This user must have at least the same rights as the remote user.
- **Other User ID:**
  User name of a SafeGuard Easy user who can assign this special right.
- **"Use Token" button**
  Click this to read the user's SafeGuard Easy password from a token if the user has logged on using a token.

The user names selected here affects the length of the Response code, which is produced later. The longer the Response code, the greater the danger that errors will occur when it is being typed and/or the user is told about it.

User ID	Length of the Response (characters)
SYSTEM	30
Issue abbreviated C/R Code	30
Other user ID	56

Remote User-ID

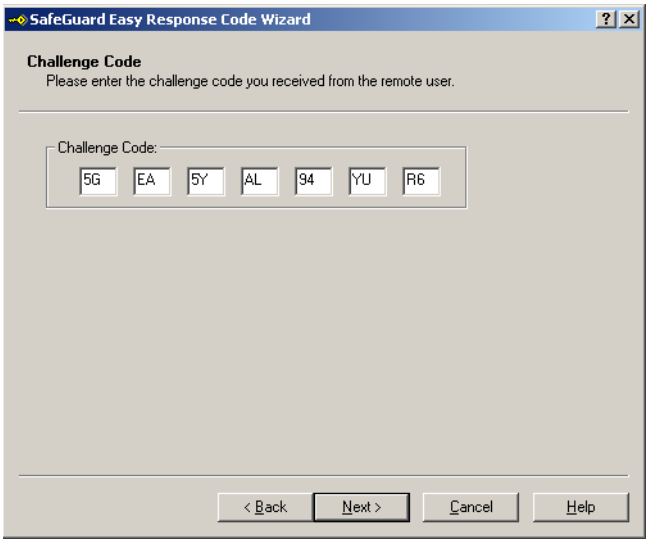
In the “Remote User-ID” dialog you see next you select the SafeGuard Easy user name of the remote user. Ask the user what access data they usually use to log on to their computer.


SafeGuard Easy Response Code Wizard
Remote User ID
Now enter the remote user's ID. Only this user will be able to use the response code.
Please select a user ID below:
Default user
Other user ID:
< Back
Next >
Cancel
Help

- **Default user:**
  User only logs on with their SafeGuard Easy password. This means that they are registered as a default user on the target system and so do not know their user name.
- **Other user ID:**
  User logs on with their SafeGuard Easy user name and password. As a result, the SafeGuard Easy user name is known. Enter it in the field.

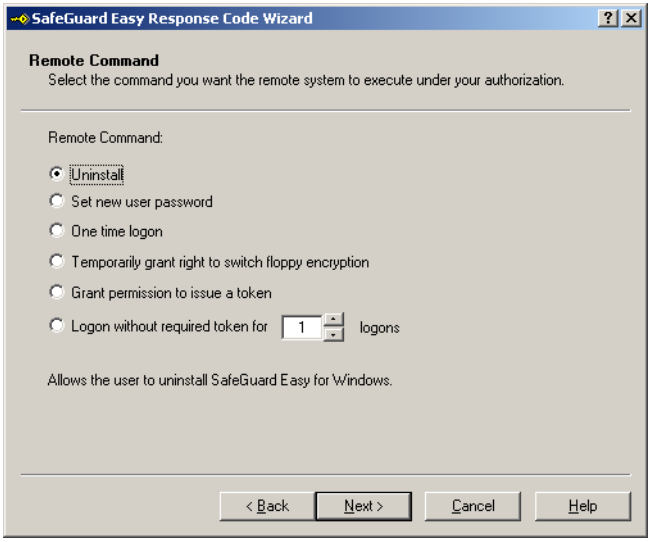
Challenge Code

In the “Challenge Code” dialog, enter the code that the remote user has told you (for example, by telephone) in the fields, which are split in pairs. The user sees the **Challenge Code** as an ASCII character string (14 characters) on their PC.



Remote Command

In the “Remote COmmand” dialog, select the **action** that the remote user should perform.


SafeGuard Easy Response Code Wizard
Remote Command
Select the command you want the remote system to execute under your authorization.
Remote Command:
Uninstall
Set new user password
One time logon
Temporarily grant right to switch floppy encryption
Grant permission to issue a token
Logon without required token for
1
logons
Allows the user to uninstall SafeGuard Easy for Windows.
< Back
Next >
Cancel
Help

One of the following actions can be carried out:

- **Uninstall**
  User can uninstall SafeGuard Easy. This type of uninstallation is only appropriate if the system administrator is not on site.

- **Set new user password**
  User can change their password, for example, if they have forgotten the old one or increased the waiting time for PBA too much by entering the incorrect password several times.

  It is not possible to assign a new password for the user SYSTEM via Challenge/Response.

- **One time logon**
  User is granted access to the affected computer for the duration of one work session (logon).

  This is a good idea if, for example, a technician is carrying out maintenance tasks.

- **Temporarily grant right to switch floppy encryption**
  The user can temporarily switch floppy disk encryption on or off for the duration of one work session. The key for floppy disk encryption must already have been set.

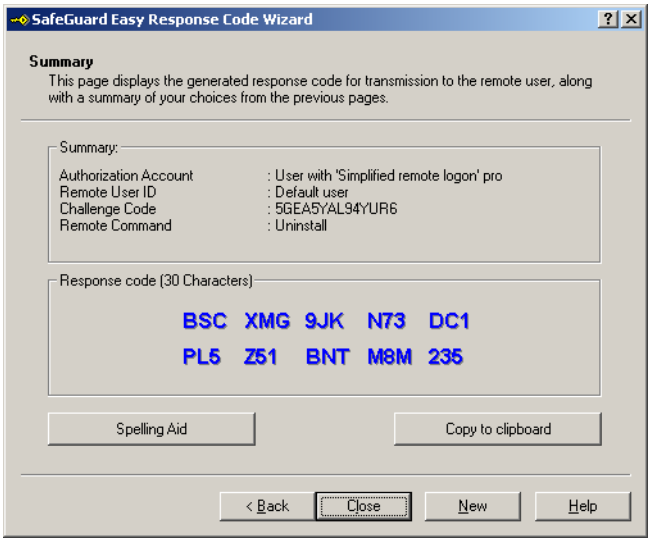
- **Grant permission to issue a token**
  The user is allowed to issue a token. This option is relevant when a token can only be issued via Challenge/Response (issue mode “external commitment“).

- **Logon without required token for "X" logons**
  The user has permission to log on without a token x times (maximum: 12). This action is used if the user has left the token at home, but needs it to access their PC.

When they confirm the data they enter, the response code is generated.

Summary

In the “Summary” dialog you see a complete overview of the settings you made in the previous dialogs in the Response Code Wizard. In addition, you see the following:


SafeGuard Easy Response Code Wizard
Summary
This page displays the generated response code for transmission to the remote user, along with a summary of your choices from the previous pages.
Summary:
Authorization Account : User with 'Simplified remote logon' pro
Remote User ID : Default user
Challenge Code : 5GEA5YAL94YUR6
Remote Command : Uninstall
Response code (30 Characters)
BSC XMG 9JK N73 DC1
PL5 Z51 BNT M8M 235
Spelling Aid
Copy to clipboard
< Back
Close
New
Help

Response code

Shows the generated response code in blue characters. This is the code you must tell to the remote user. The remote user enters the response code in the fields intended for that purpose. The response code is only valid once! A new one must be generated for each request.

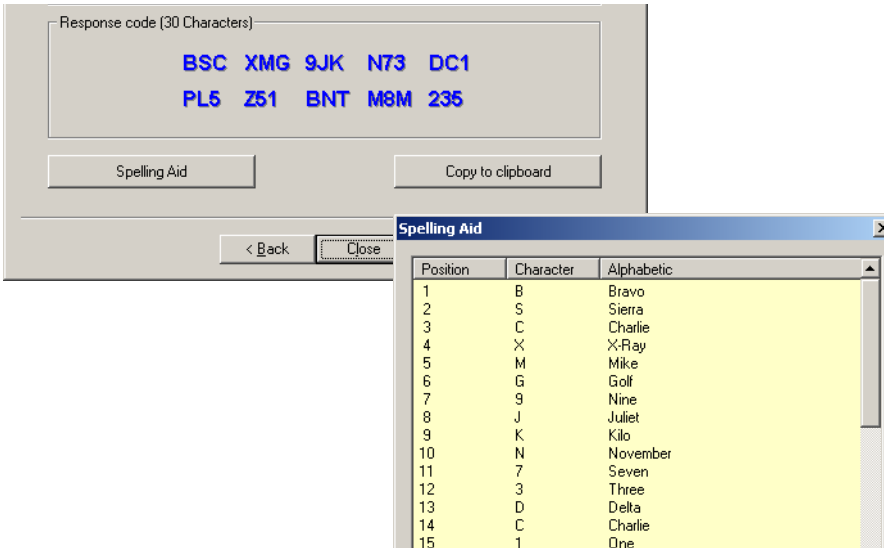
Copy to clipboard

Copies the response code to the Clipboard from where you can paste it into any text editor. With this feature you can, for example, simply send the response code to the user via SMS or e-mail.

If all entries are correct and the user can perform the necessary actions, you close the Response Code Wizard by clicking on **Close**. If you click **New**, all entries are deleted, and you can generate a new/additional response.

Spelling Aid
To make it easier to pass on the code to the user, and reduce errors, there is a Spelling Aid in the Response Code Wizard.

When you click the [Spelling Aid] button, you see a window split into three columns with different column headers. Under "Position" you see the position of the character within the code. As a result, questions can be answered immediately without spending a lot of time (counting the number of characters from the start, etc.). You can see which character to say in the code which has the same name. "Alphabetic" shows which word the character can be "linked" with, to prevent misunderstandings, such as standard radio code words (in this example). Usually words whose first letters are entered in the code fields are used. The actual response code is already displayed in the window. You simply need to read it from top to bottom.



26.4 Optional extensions of the Challenge/Response concept

There are various software and hardware-based extensions of the Challenge/Response procedure.

26.4.1 Helpdesk Console

In large IT environments, where the helpdesk employees themselves should not know the master passwords of the clients, there is the option of extending the system with a cryptographic hardware module (CryptoServer) and a software based solution.

Hardware-based Helpdesk Console

When CryptoServer 2000 is in use, the SafeGuard Easy Administrator passwords are entered once in the CryptoServer 2000 and are stored there securely. The helpdesk team do not know these passwords.

The response code is then generated within CryptoServer 2000 itself. This allows the Helpdesk team to generate a response code for the user data (name, challenge code) they have been given without knowing the SafeGuard Easy administrator's password. The CryptoServer 2000 system administrator gives each member of the Helpdesk staff an account (user name, password) on the CryptoServer with which they can generate a response code. This account can be deleted at any time (for example, if a member of staff leaves the company), to ensure that this person can no longer access CryptoServer 2000.

The hardware-based Helpdesk Console is available as a separate add-on.

Central Helpdesk Console

The Central Helpdesk Console works similarly to the hardware-based CryptoServer solution. In this scenario the helpdesk employees themselves also do not know the master passwords of the SafeGuard Easy clients.

With the software-based Central Helpdesk Console the information necessary for creating a response, is stored in a database that is protected (encrypted with AES-256) on a machine on which the Internet Information Services run. There the response code corresponding to given challenges is computed and displayed to the helpdesk employee. The helpdesk staff members authenticate individually and remotely against the web page on the Internet Information Server.

The Central Helpdesk Console is available as separate add-on.

26.4.2 Web Self Help

The main benefit of the SafeGuard Easy self help solution is that it enables ordinary SafeGuard Easy users to help themselves if they have forgotten their SafeGuard Easy password. To reset a forgotten password users must register themselves in a central database. Registration is performed using a special mechanism: users enter answers to freely selectable questions. These answers are stored in the database. After registration the user receives a confirmation mail with a PIN. As soon as the user wants to create an Response code for their registered SafeGuard Easy profile they must enter the PIN and the correct answers.

To make the self help feature available from almost anywhere, the solution is based on web technology and does not require any additional software to be installed on the client

Self help is also available as separate add-on.

26.4.3 VOICE.TRUST

Another possible extension of the Challenge-Response System is to set up a biometric server from VOICE.TRUST with plug-in modules for SafeGuard Easy or SafeGuard PDA. The VOICE.TUST server is able to authenticate calling users via their voice (Voiceprint) and perform the complete challenge/response procedure with the user automatically via voice recognition and synthesis 24 hours a day. The human helpdesk staff are only needed in exceptional cases, and so are no longer forced to waste their time on routine work like resetting forgotten passwords.

Please contact your local SafeGuard Easy supplier for information about the optional extensions.

27 Creating emergency media and saving the system kernel

If your computer has an encrypted hard disk, and SafeGuard Easy error messages appear, it is usually because it was not possible to find the SafeGuard Easy system kernel. The system kernel contains the drivers for SafeGuard Easy and the master boot record.

Errors can often be resolved quite simply by loading a pre-saved version of the current system kernel. However, to load the system kernel the users must have both an intact system kernel and an **emergency medium (floppy disk, CD or USB memory stick)**. This emergency floppy disk contains the backup system kernel and files that will help you resolve SafeGuard Easy errors.

However, if a system error occurs it is probable that you will not be able to access the hard disk. You should therefore always store the system kernel and emergency files on a floppy disk or another form of removable medium.

NOTE:
You will find more information on this subject in the Utimaco Knowledge Database http://www.utimaco.com/myutimaco.

Use the Knowledge database's "Search" field to look for key words like "Emergency" or "Emergency Disk".

27.1 How to create an emergency floppy/system kernel backup

The emergency floppy disk is created by the "Emergency Disk Wizard", which is present after every standard installation on a client. If the floppy disks/removable media drives are encrypted, encryption is switched off while the emergency floppy disk is being created.

This means that the emergency floppy disk always has the most up-to-date version of the system kernel. Any significant change, such as a change to the encryption status, should always be backed up to this floppy disk. You can configure an option in the Emergency Disk Wizard to prompt the user to back up the system kernel at regular intervals. This must then be copied to the emergency floppy disk.

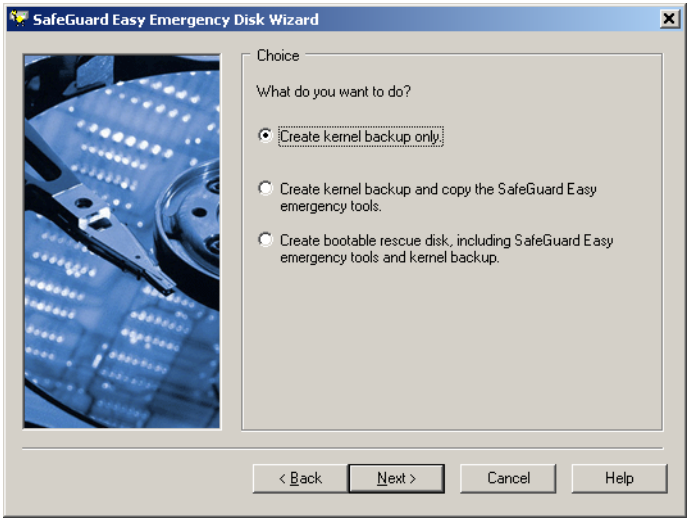
The wizard has an additional option for creating a bootable emergency floppy disk that contains the system kernel, emergency tools and driver files for the keyboard layout.

27.1.1 Running the emergency disk wizard

The Emergency Disk Wizard starts automatically after the first restart after SafeGuard Easy has been installed. However, you can also run it by selecting **Programs/Utimaco/SafeGuard Easy/Emergency Disk Wizard.**

You confirm correct entries in the wizard by clicking [Next].

1. Once the wizard has started, a second dialog appears. In this dialog you specify which files are to be saved to the emergency floppy disk.

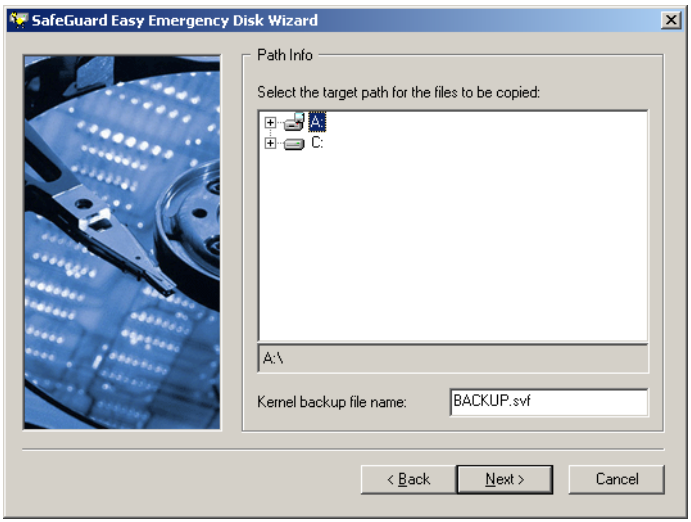

SafeGuard Easy Emergency Disk Wizard
Choice
What do you want to do?
Create kernel backup only
Create kernel backup and copy the SafeGuard Easy emergency tools.
Create bootable rescue disk, including SafeGuard Easy emergency tools and kernel backup.
< Back
Next >
Cancel
Help

There are the following options here:

- **Create kernel backup only**
  This function saves the entire system kernel (driver for SafeGuard Easy and the Master Boot Record) in one file.
- **Create kernel backup and copy the SafeGuard Easy emergency tools**
  Saves the system kernel and SafeGuard Easy's emergency files

- **Create bootable rescue disk, including SafeGuard Easy emergency tools and kernel backup**
  Creates a boot floppy disk with a version of FreeDOS, the system kernel and emergency files.

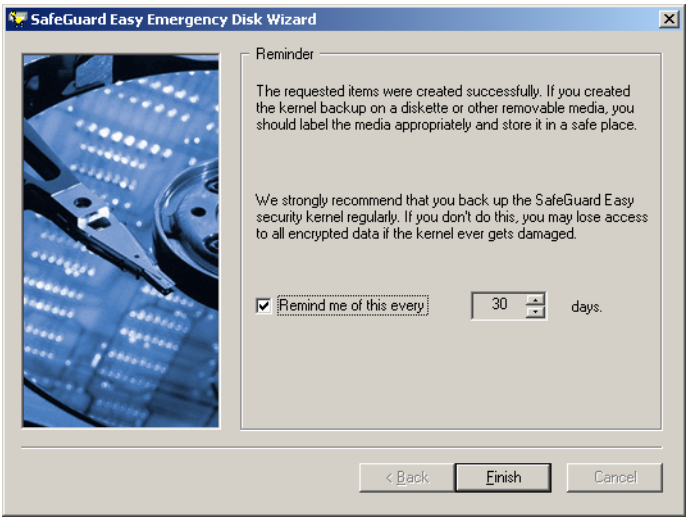
2. Now select where the data (system kernel and emergency files) is to be saved.



In the *Path Info* field you can define where the system kernel and emergency files (if selected) are to be saved. Enter a name for the system kernel in the *Kernel backup file name* field. The default setting is `BACKUP.svf`, but you can change the name and the .svf extension if required. You can also save the system kernel to the hard disk or a network drive.

However, if a system error occurs it is probable that you will not be able to access the hard disk. You should therefore always store the system kernel and emergency files on a floppy disk, another form of removable media or the network drive.

3. In the *Reminder* dialog you can specify how often you would like to be reminded to carry out a system kernel backup.


SafeGuard Easy Emergency Disk Wizard
Reminder
The requested items were created successfully. If you created the kernel backup on a diskette or other removable media, you should label the media appropriately and store it in a safe place.
We strongly recommend that you back up the SafeGuard Easy security kernel regularly. If you don't do this, you may lose access to all encrypted data if the kernel ever gets damaged.
Remind me of this every
30
days.
< Back
Finish
Cancel

Because it is vital that you have the most up-to-date version of the system kernel available to use if system errors occur, we strongly recommend that you carry out regular backups.

27.1.2 Using the command line to save the system kernel

You can also save the system kernel from the command line by typing

```
SGEBACK.EXE /f:<Path/Filename> | /S | /?
```

/f:	Shows the path and file name used to save the kernel. You can select any name and extension for the target file.
/S	Sends the kernel backup defined in the /f parameter to the SafeGuard Easy Server
/?	Shows this help message

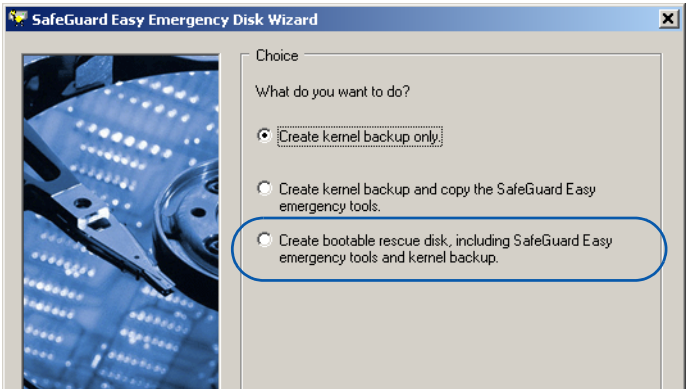
27.1.3 How to save SafeGuard Easy emergency files to floppy

You can also save the emergency files to a floppy "manually". Copy the following files from SafeGuard Easy's installation folder:

- SGEASY.exe
- Sgeasy.hmf
- Sgecrypt.mod
- Sgenls.mod
- sgekrnl.mod

27.2 How to create a bootable emergency disk

In addition, the Emergency Disk Wizard gives you the option of creating a bootable start floppy that includes a system kernel, emergency tools and driver files for the keyboard layout. This is an easy way of combining a boot floppy and a SafeGuard Easy emergency floppy.


SafeGuard Easy Emergency Disk Wizard
Choice
What do you want to do?
Create kernel backup only
Create kernel backup and copy the SafeGuard Easy emergency tools.
Create bootable rescue disk, including SafeGuard Easy emergency tools and kernel backup.

How to create a bootable emergency diskette:

1. Insert a formatted floppy and start the Emergency Disk Wizard.

2. Select the "Create bootable rescue disk, including SafeGuard Easy emergency tools and kernel backup".

We recommend that, the first time you save the system kernel, you create a bootable start floppy, and only update the system kernel if it is changed.

27.3 How to create a bootable emergency CD

Nowadays, mobile devices like notebooks no longer have floppy drives. For this reason you can also start SafeGuard Easy from a CD in an emergency.

How to create a bootable emergency CD:

1. Save the boot image file `Floppy.iso` (from the \TOOLS directory) to the hard disk and use any commercially-available CD burner to save the file to CD.

   The ISO file contains the entire boot floppy, as it was created by the Emergency Disk Wizard, apart from the system kernel backup.

2. Use the "Emergency Disk Wizard" to create a system kernel backup. Save the system kernel backup either on the CD itself or on an external plain text (unencrypted) medium that you can access in an emergency.

Check in BIOS that your system (PC) boots from CD.

Whether or not an emergency boot from CD can be performed successfully depends on the workstation's BIOS support!

27.4 How to create a bootable emergency USB memory stick

The USB stick must be bootable on your system!

Follow these steps to create a bootable emergency USB stick:

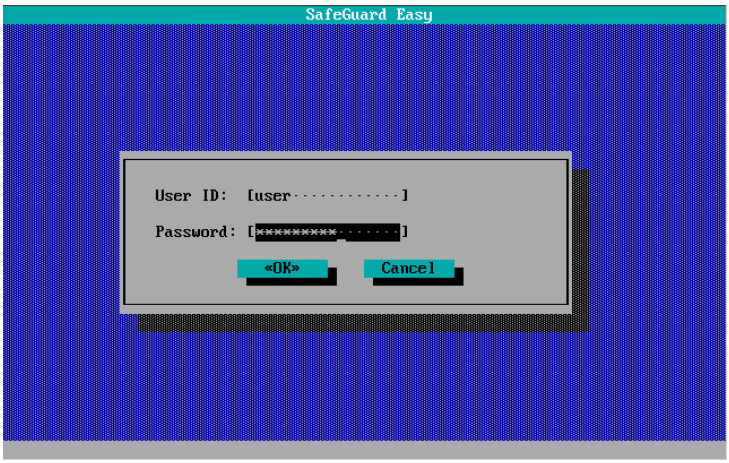
1. Make the memory stick bootable.
2. Copy the SafeGuard Easy emergency files to your memory stick.
3. Run SGEasy.exe.

The workstation's BIOS support determines whether an emergency boot from USB memory stick can be performed successfully!

27.5 Performing an emergency boot

If a system error occurs on an encrypted hard disk, proceed as follows:

1. Insert an emergency floppy/CD and start the PC.
2. The `Sgeasy.exe` emergency program runs unattended.
3. Enter the SafeGuard Easy password. Click [OK] to confirm the password.



4. You now see a menu with the options *Uninstall, Backup, Restore*, and *Repair*.

27.5.1 Restoring a system kernel

You can only restore the system kernel if a valid system kernel is already present on the workstation. If there is a backup copy, the MBR (master boot record) and the SafeGuard Easy system kernel are simply restored using this data backup on the PC.

This function ***must not*** be executed if

- SafeGuard Easy was previously uninstalled
- the system kernel backup is not the most up-to-date version. This would be the case if, for example, the encryption status of the hard drive(s) was changed between the backup and the restoration.

All SafeGuard Easy users (not only "SYSTEM" users) can restore a system kernel.

27.5.2 Repairing the system kernel

In contrast to the "Restore" option, a repair can also be carried out without using a backup copy of the system kernel. The repair function searches the entire hard disk for the SafeGuard Easy system kernel and attempts to restore it (with no guarantee of success!).

This function is only necessary if

- no system kernel backup exists
- the emergency file is not the most up-to-date version. This would happen if the encryption status of the hard disk(s) was changed between the system kernel backup and the time the system error occurred.

If you select "Repair" a diagnostics routine attempts to find the system kernel and reactivate it. This may take several minutes. Progress is shown in a progress bar. You are then informed whether the repair has been successful.

> ***NOTE:***
> Attempts to resolve a system error with "Repair" are not always successful. For this reason, you should always have a current backup of the system kernel.

27.5.3 Emergency uninstall of SafeGuard Easy

If the system error cannot be resolved either with "Restore" or "Repair", the only remaining alternative is option three, to decrypt the hard disk and switch off PBA. After uninstalling SafeGuard Easy, the workstation reboots twice automatically.

However, before you can do this, the SafeGuard Easy user profile must have the appropriate rights. If a user does not have uninstall rights, they can be assigned to the use via the Challenge/Response procedure (see 'Remote maintenance (Challenge/Response)').

You should also carry out a data medium check in Windows. You will find more information about this in your Windows documentation.

Failed decryption

Please contact our support team if the initial encryption or the decryption fail for any reason.

Extended forensic support (/NoReboot parameter)

SafeGuard Easy's emergency decryption now includes the `/NoReboot` command line parameter for the `Sgeasy.exe` emergency program. You use this command line parameter to prevent an automatic restart after emergency decryption. This is useful for performing a forensic analysis of the hard disk.

Process:

1. Booting the emergency medium.
2. Run `Sgeasy.exe /NoReboot`.
3. The emergency decryption/deinstallation ends.
4. The PC is stopped and the system displays an information text. In this state it is not possible for a program to run or for a user to enter anything.

Hard disk is defective.

Please note: if you suspect that your encrypted hard disk is physically damaged we recommend that you do not decrypt it using an emergency data medium.

You will notice if your hard disk has a physical defect because it may make rattling or clicking noises or no longer be recognized by your PC's BIOS. In this situation, do not make any more rescue attempts on your own: contact the specialists. They will try to transfer the contents of the corrupted hard disk onto an intact disk so that emergency decryption can be performed on the data. Obviously, getting outside help will mean additional costs, so you will need to decide how valuable the data on the defective hard disk is to you.

> ***NOTE:***
> You will find more information on this subject in the Utimaco Knowledge Database http://www.utimaco.com/myutimaco.
>
> Use the Knowledge database's "Search" field to look for key words like "Data Recovery".

27.5.4 Notes

- **System kernel storage location**
  If the Windows boot partition is not on the first hard disk the SafeGuard Easy system kernel is automatically saved to the C: partition during installation. As a result, after SafeGuard Easy has been installed, you should not format this partition again because it contains the most important Windows information (system kernel, drivers, etc.). However if you do format it after installation, you must re-install the entire system.

  The kernel backup is, however, a system-specific backup, i.e. it can only be restored on the same PC as it was initially saved.

  However, if a system error occurs it is probable that you will not be able to access the hard disk. You should therefore always store the system kernel and emergency files on a floppy disk, another form of removable medium, or the network drive.

- **Language settings for the emergency program Sgeasy.exe**
  The language of the emergency program's user interface is defined by the Sgeasy.hmf file (which you will find on the emergency floppy disk).The different versions of the language file, for English (Sgeasy09.hmf.), French (Sgeasy0C.hmf), and German (Sgeasy07.hmf.), are stored in the SafeGuard Easy installation folder. The user must rename the particular SGEASY file they require <09,07,0C>.hmf for the emergency floppy disk to SGEASY.HMF before they can use SGEASY.EXE in the language they want.

27.6 Accessing encrypted data when booting from an external medium

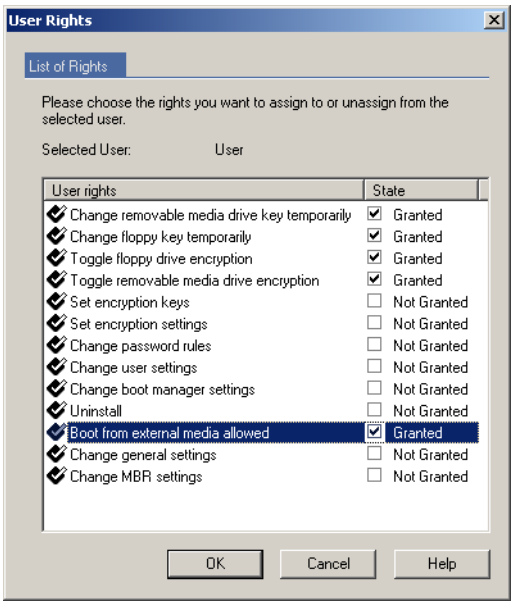
In some (emergency) situations users want to be able to start a SafeGuard Easy encrypted system from an external medium, for example, to access data on the workstation if the operating system on the workstation does not run anymore. To boot from an external medium (and accessing data in plain text) users must authenticate themselves with valid SafeGuard Easy user data in the Pre-Boot Authentication.

This method can be a good way to save data before repairing the operating system or emergency uninstalling SafeGuard Easy.

In addition to MS DOS/Windows 9x boot floppies, a system encrypted with SafeGuard Easy can be booted from boot CDs or bootable USB memory sticks (DOS and WIndowsPE). It is important that the external boot medium contains SafeGuard Easy's drivers.

27.6.1 Prerequisites

Please keep in mind that booting from an external medium after PBA-Authentication is an administrative right, which by default is only assigned to the “SYSTEM” account. To start a workstation from an external medium the SafeGuard Easy user profile which is logged on in the PBA needs the right "Boot from external medium allowed".



27.6.2 Procedure

1. Boot the system from hard disk.
2. The SafeGuard Easy Pre-Boot Authentication appears.
3. Enter data in PBA.
4. a) Insert the **boot floppy**. Press **[Enter]** to confirm PBA data.
   b) Insert the **boot CD**. Press **[F7]** to confirm PBA data.
5. PC boots from the external boot medium.
6. After a reboot access or save data.

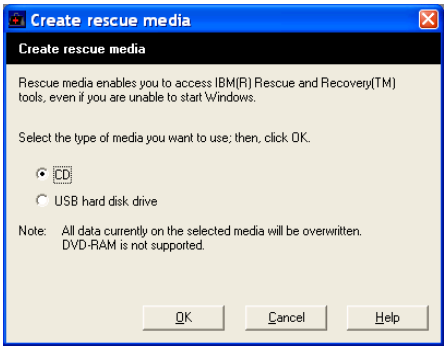
27.6.3 Notes

- The workstation's BIOS support determines whether an emergency boot from CD or USB memory stick can be performed successfully!
- In our Knowledge Database you will find a description of how to create a bootable Windows PE CD.

  You will find more information on this subject in the Utimaco Knowledge Database http://www.utimaco.com/myutimaco.

  Use the Knowledge database's "Search" field to look for key words like "BartPE" or "SGE".
- If SafeGuard Easy is installed Lenovo's Rescue and Recovery Feature "Create Rescue Media" automatically creates a CD including SafeGuard Easy drivers. You can access this feature via Programs /ThinkVantage (Access IBM)

  .


Create rescue media
Create rescue media
Rescue media enables you to access IBM(R) Rescue and Recovery(TM) tools, even if you are unable to start Windows.
Select the type of media you want to use; then, click OK.
CD
USB hard disk drive
Note: All data currently on the selected media will be overwritten. DVD-RAM is not supported.
OK
Cancel
Help

27.6.4 What should I do, if ...

... booting the system from external media fails?

This may occur for the following reasons:

- The logged-on SafeGuard Easy user does not have the SafeGuard Easy right "Boot from external media allowed".
- Hard disk drive encryption has been started but is not yet complete.

Additional reasons for a failed floppy boot:

- The floppy drive is not called by the default floppy controller but the USB interface.
- The floppy drive is encrypted while the boot floppy is not.

28 Displaying SafeGuard Easy system status

SafeGuard Easy has a command line tool called SGEState with which you can display the current status of a SafeGuard Easy installation on a user PC (version, encryption mode, encrypted/not encrypted etc.). This tool is particularly suitable for installations in large environments, since it provides an easy way for an administrator to check the status of a SafeGuard Easy installation.

However, you can also implement SGEState in such a way that particular activities/processes are not executed until the SafeGuard Easy installation process (or the encryption process) has completed.

After the SafeGuard Easy Client package has been installed, you will find SGEState in the SafeGuard Easy program folder.

28.1 Reporting

SGEState can also be used for reporting:

- The SGEState return code can be evaluated on the server using third-party management tools.
- SGEState /LD produces output that is formatted for LANDesk (and some other products). This output is diverted to a file and can be sent to the server for evaluation.

28.2 Parameters

You can call SGEState with these parameters:

```
SGESTATE [/?] [/Q | /L | /LD] [/E [/Mvalue]] [/Dvalue] [/R]
```

SGEState /? gives you an overview of all available command line parameters.

```
/Q...Quiet mode: No output, program ends with return code:

  0...SafeGuard Easy not installed.
  2...SafeGuard Easy installed.
  3...SafeGuard Easy installed. Encryption or decryption process active.
255...An error occurred during the check. In this case, a message
      to the console will state the nature of the problem.

/L...Loud mode. Will display details to the console including:

Operating System: [WINDOWS 2000 ¦ WINDOWS XP ¦ WINDOWS SERVER 2003]

Installation Status         : [INSTALLED ¦ NOT INSTALLED ¦ UNKNOWN ¦
                               INSTALLED (NOT READY FOR BACKUP)]
Version number              : [N/A ¦ number]
Installation Mode           : [N/A ¦ STANDARD ¦ PARTITIONED ¦ BOOT PROTECTION ¦
                               UNKNOWN]
Disk Encryption             : [N/A ¦ OFF ¦ ON]
Floppy Encryption           : [N/A ¦ OFF ¦ ON]
Removable Media Encryption  : [N/A ¦ OFF ¦ ON]
Initial Encryption          : [N/A ¦ ACTIVE ¦ INACTIVE]

Pre Boot Authentication     : [N/A ¦ OFF ¦ ON]
Current Authentication      : [N/A ¦ USER ¦ WAKE ON LAN]
Secure Auto Logon           : [N/A ¦ OFF ¦ ON]
Secure Smartcard Auto Logon: [N/A ¦ OFF ¦ ON]
SGE Management Server       : [N/A ¦ <UNMANAGED> ¦ OFFLINE ¦ server]

Return code                 : [ReturnCode]

/LD...The details are displayed in LANDesk mode:

/E...Extended return code:

En-/Decryption in process          :  1
SafeGuard Easy installed           :  2
Floppy Encryption "ON"             :  4
Disk Encryption "ON"               :  8
Installation Mode "Boot Protection": 16 (hex 10)
Installation Mode "Partitioned"    : 32 (hex 20)
Installation Mode "Standard"       : 64 (hex 40)
                                     only one mode is possible, (16, 32 or 64)

/Mvalue...value mask for extended return code 1..127

For example: SGESTATE /E produces return code 43 (hex 2b). This indicates:
Partitioned mode, Disk Encryption "ON", SGEasy installed, Encryption in process

For example: SGESTATE /E /M15 produces return code 11 (hex 0b)

/Dvalue...value for desired return code 0..127
         The return code is computed until the desired one is reached
         Calculation can be stopped by pressing any key

/R...the return code is stored in the registry

The input charaters are not case sensitive.
```

29 Auditing

Recording incidents that have security implications is a prerequisite for detailed system analysis. By examining the logged events it is possible to understand procedures on a workstation or within a network more exactly. For example, logging can be used to prove that unauthorized users have impacted security. Logging also helps the system administrator to find incorrectly-denied user rights and correct them.

Auditing logs events that installed SafeGuard products trigger, such as whether a user has logged on with a smartcard, whether a PIN has been changed, a certificate has expired, etc.

A user with the appropriate rights can either view the logged events directly, via the Windows event viewer, or they can export them to a custom file for archiving. Data can either be logged locally or sent to a central workstation via a remote log.

In addition to pure logging, Auditing includes a filter mechanism that supports you in selecting relevant events.

The following SafeGuard Easy events are involved in logging:

- The carrying out of logon to PBA (successful/failed)
- Administrator tasks (create a user etc.)
- Processes involved in central administration (assign client to server etc.)
- Successful/failed execution of configuration files.
- Installation/removing processes
- Encryption/decryption processes

29.1 How to use Auditing

Auditing is a user-friendly solution for recording events. The examples below show some typical scenarios in which Auditing is used.

Central monitoring of workstations in a network

For example, the administrator will need to be regularly informed about security-critical SafeGuard events (such as the running of files for which a user has no permission, etc.). The administrator can configure Auditing in such a way that, if these SafeGuard events occur on particular computers, they are automatically passed on to the event viewer, or a custom log file on a specific workstation, and saved. In this way the processes on different workstations can be continually checked without staff having any influence on the recording of log data. To use this mechanism, it is necessary to use the Microsoft Message Queuing components.

Monitoring mobile users

Mobile users are usually not constantly linked with the corporate network.

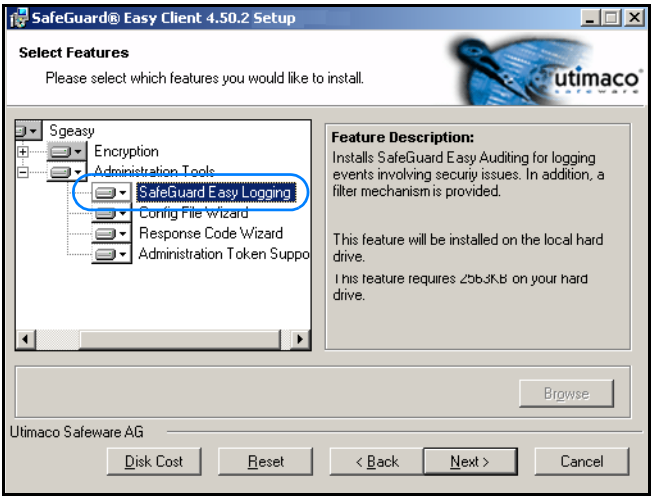
For example, external service engineers may remove their notebook from the network for a meeting. As soon as they log onto the network again, Auditing is used to transfer the SafeGuard events that were logged during the time that the user was off the network. In this way Auditing provides the administrator with an accurate overview of the user's activities during the time that the relevant computer was not connected to the network.

29.2 Installing Auditing

To install SafeGuard Easy Auditing activate the feature SafeGuard Easy Logging during SafeGuard Easy Client installation.

1. Run `Sgeasy.msi` from the Client folder of the product CD.

2. When the “Select Features“ dialog is displayed activate “SafeGuard Easy Logging“, along with the already-selected components and continue the installation.



3. After you have finished the installation, restart your computer.

29.3 Configuring Auditing

All settings for Auditing are administered via group policies/group policy objects with the help of the **Group Policy snap-in** in the **Microsoft Management Console (MMC)**. By default the MMC is integrated into Windows 2000 and Windows XP.

Follow these steps to add the Group Policy snap-in:

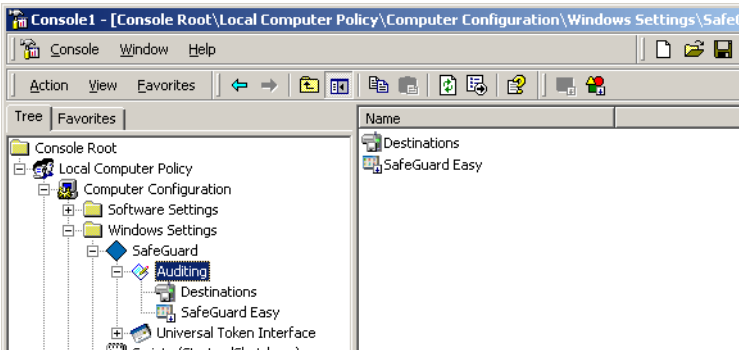
1. Call the Microsoft Management Console (select Start, Run..., and then type "mmc".)

2. The MMC is displayed. Open the *Console* menu, select *Add/Remove Snap-in* and click [Add].

3. Double-click the Group Policy snap-in.

4. Select Local Computer (Console is valid for the local machine) or press the [Browse] button in an Active Directory environment to select a group policy object.

The Auditing folder will be displayed under User and Computer configuration in the Windows settings.



29.4 Configuring Event Logging

To log the events, carry out these steps in this sequence:

- Define Destinations where the events are to be output
- Configure the events that are to be recorded
- View the logged data

29.4.1 Defining destinations

The failed or successful execution of events is documented in output modules. Auditing calls these output modules *destinations*. A destination can be Windows' own event viewer or a log file that you select yourself. Events on one workstation can also be logged remotely on another workstation. Auditing only writes those events that are linked with an Utimaco product to a destination.

Event Viewer
The Windows event viewer is a tool that is used to log monitoring information. The event viewer can display and manage protocols for system, security and application events. It can also save these event logs.

Log File
For archiving purposes, SafeGuard events can be processed and evaluated with a wide range of tools (for example, MS Excel).

Remote Log
The task of the remote log is to exchange data between one destination workstation and a remote workstation in the network. To do this, the destination computer collects information (events) in its event viewer or a log file. This information is then transferred from the remote workstation via remote logging. **Remote Log only works if SafeGuard Advanced Security's Base Module is installed.**

NOTE:

To exchange log data between several workstations we recommend that you use the remote log mechanism instead of directly writing the data to a log file on a public network drive.

The remote log procedure must be used for creating logs on a Windows NT server because the system account that Auditing works with has no network credentials and therefore cannot be written to a log file that has been specified on a network drive.

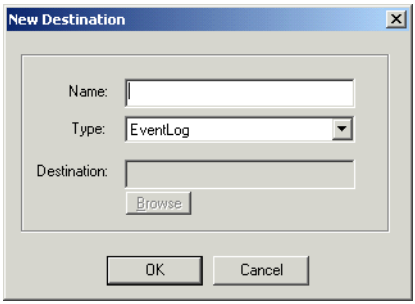
29.4.2 Creating a new destination

Follow these steps to add a new destination:

1. Click **Destination**.

2. Click the icon or right-click **Destinations**, then select **Add new destination**.

3. The New Destination dialog appears.



Name:
Name of the destination. The name can contain spaces and special characters.

Type:
Defines the type of logging to be used:

- Select **Eventlog** if you want the events to be logged in the Windows event viewer.
- Select **Logfile** if you want the events to be logged in a particular file.

  Hint: the file must not be write-protected.

- Select **Remote Log** if you want the events to be logged on a remote workstation.
  Only available in combination with SafeGuard Advanced Security's Base Module!

Destination:
Click the [Browse] button. Select the log file or, in the case of RemoteLog, the workstation on which the events are to be logged.

You can create an unlimited number of destinations.

29.4.3 Removing a destination

If a destination is no longer required, you can remove it. Right-click the destination you want to remove, select the Delete command, and confirm deletion at the prompt you see next.

> ***NOTE:***
> You can remove destinations that are still in use! To avoid problems, a warning is displayed.
>
> If a destination is deleted, all events connected with this destination will be "Deactivated".

29.4.4 Copying a destination

Destinations can be copied between Group Policy Objects (GPOs)

- via the copy & paste commands on the Auditing context menu
- with drag & drop.

If you copy destinations then all the destinations already located there will be automatically removed.

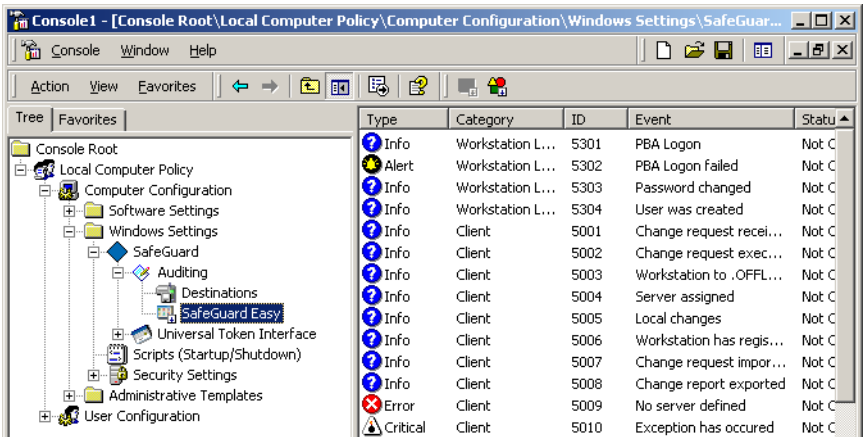
29.5 Selecting events

The Auditing node contains different folders that contain pre-defined events for each of the installed Utimaco products:

Follow these steps to configure the auditing of the product's events:

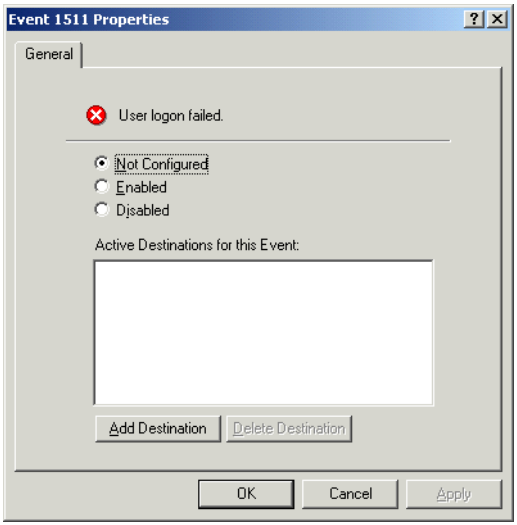
1. Click one of the folders in the Auditing node.

2. The different events are displayed on the right. Click a column heading to sort events by this heading.
   You can sort according to Category, Type, Event, Status or Destinations.



3. Double-click an event or right-click it and select Properties.

4. You assign the status and destination in the Properties dialog.



Status

- **Not configured (Default)**: Event is disabled and not recorded.

  WARNING:
  Defined destinations have priority over these settings. If a destination has already been assigned to an event, this option is no longer relevant.

- **Enabled:**
  Event is enabled and recorded.

- **Disabled:**
  Event is disabled and not recorded.

Active Destinations for this Event

- [Add Destination] opens a dialog that displays all registered destinations. Select one or more of these destinations. After you click [OK], the destinations are displayed in the *Active destinations for this event* field.
- [Delete Destination] removes destinations.

5. Click [Apply] and [OK].

Multi-selection

You can also select several events/destinations at once. Press the [Ctrl] and [Shift] buttons simultaneously. You can then select several events with a single mouse-click. Right-click one of the selected events to open it. In the context menu, select *Properties* and define status and destination. The settings will be applied to every event you select after clicking on [OK].

29.5.1 Configuring all events

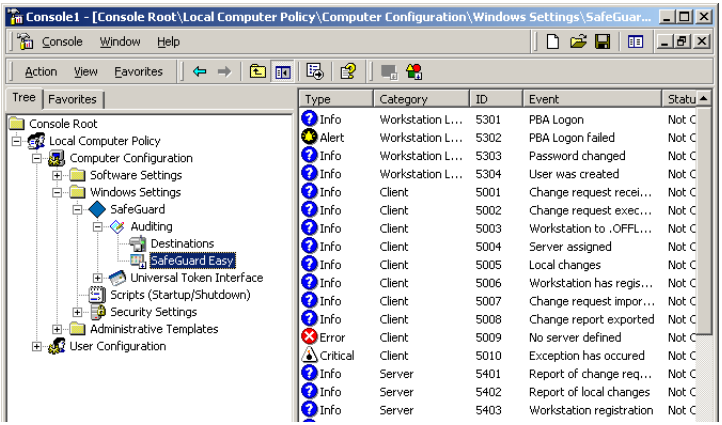
You use the **Configure all events** command to configure all the events present in one folder in a single step.

Select the Auditing folder or any another subfolder. Then select Configure all events in the context menu.

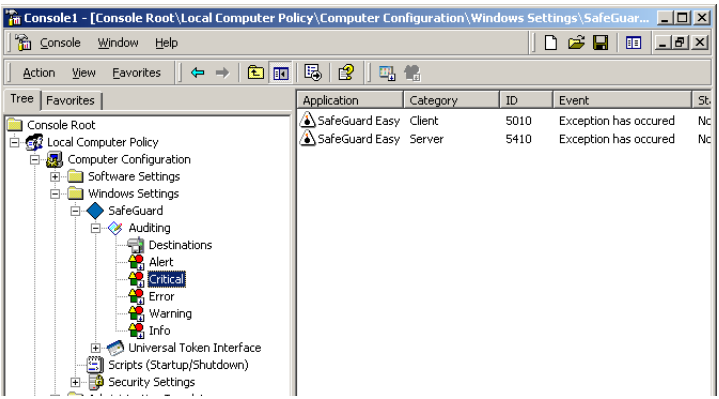
Enter the status and active destinations in the All events Properties dialog. Click [Apply]. The selected settings apply to all events.

29.5.2 Changing the view

By default events are sorted by SafeGuard application.


Console1 - [Console Root\Local Computer Policy\Computer Configuration\Windows Settings\SafeGuar...
Console Window Help
Action View Favorites
Tree Favorites
Console Root
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
SafeGuard
Auditing
Destinations
SafeGuard Easy
Universal Token Interface
Scripts (Startup/Shutdown)
Security Settings
Administrative Templates
User Configuration
Type Category ID Event Statu
Info Workstation L... 5301 PBA Logon Not C
Alert Workstation L... 5302 PBA Logon failed Not C
Info Workstation L... 5303 Password changed Not C
Info Workstation L... 5304 User was created Not C
Info Client 5001 Change request recei... Not C
Info Client 5002 Change request exec... Not C
Info Client 5003 Workstation to .OFFL... Not C
Info Client 5004 Server assigned Not C
Info Client 5005 Local changes Not C
Info Client 5006 Workstation has regis... Not C
Info Client 5007 Change request impor... Not C
Info Client 5008 Change report exported Not C
Error Client 5009 No server defined Not C
Critical Client 5010 Exception has occured Not C
Info Server 5401 Report of change req... Not C
Info Server 5402 Report of local changes Not C
Info Server 5403 Workstation registration Not C

Using the filter mechanism you can sort events according to their warning level, independent of the application that triggered them (for example, all critical events).



You change the view by selecting these icons: and .

29.6 Viewing audited events

Event messages are recorded in the event viewer or in a log file.

The audited events display the following settings:

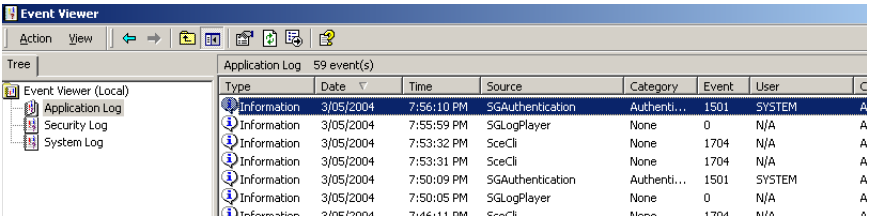
- Computer: Name of the computer on which the event occurred.
- Date: Current date of the computer that caused the event.
- Time: current time on the computer that caused the event.
- User: Name of the user who was logged on when the event occurred.
- Type: Windows classification level of the event, e.g. error, warning, information.
- Event ID: Number that is assigned to every event. This can be any number between 0 and 0xffffffff (e.g. 4 294 967 295).
- Source: Application recording the event, e.g. SGPWC = Password restrictions.
- Category: Classification of the event according to the classification models of the source that produced the event.

The system settings (regional options) define the language of the audited events.

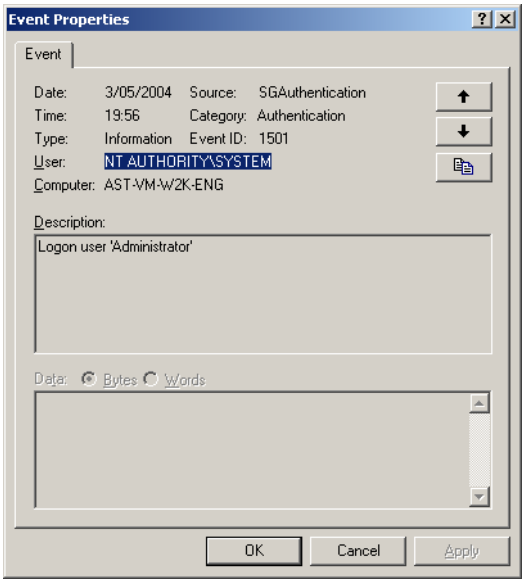
29.6.1 Event Viewer

Auditing records audited events in the Event viewer's Application Log.

To run the Event viewer, click Start, select Programs, select Administrative Tools and then click Event viewer. In the console tree, click the Application Log. The events are displayed in the details window. Click the event you want, and then on the Action menu properties.


Event Viewer
Action View
Tree
Event Viewer (Local)
Application Log
Security Log
System Log
Application Log 59 event(s)
Type Date Time Source Category Event User
Information 3/05/2004 7:56:10 PM SGAuthentication Authenti... 1501 SYSTEM
Information 3/05/2004 7:55:59 PM SGLogPlayer None 0 N/A
Information 3/05/2004 7:53:32 PM SceCli None 1704 N/A
Information 3/05/2004 7:53:31 PM SceCli None 1704 N/A
Information 3/05/2004 7:50:09 PM SGAuthentication Authenti... 1501 SYSTEM
Information 3/05/2004 7:50:05 PM SGLogPlayer None 0 N/A

Double-click the event to display more detailed information.



NOTE:
By logging events to the Application Log via remote log, the computer name, date and time displayed in the Event's properties dialog represent the data of the workstation which recorded the events. The data of the workstation that initiates an event is displayed in the Description field.

The Windows event viewer does not show all Auditing's Message Types. The table shows how Auditing's events are displayed in the Event viewer:

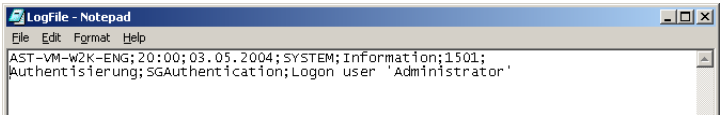
SafeGuard Auditing	**Event Viewer**
Emergency Alarm Error Critical	Error
Warning	Warning
Notice	Notice
Information	Information

29.6.2 Log file

An Auditing log file is equivalent to the Windows log file. However, only the events caused by an Utimaco product are recorded in an Auditing log file. The events are shown in chronological listing. You can export the log data using “Save As“ and, for example, convert and evaluate it in a database program.

> ***NOTE:***
> Do not use files which are EFS-encrypted or located in a folder which is EFS-encrypted.

Example of a log file:



The log file entries represent the following settings:

AST-VM-W2K-ENG	Computer name
20:00	Time
03.05.2004	Date
System	Specifies a user or a group who creates this event.
Information	Warning level
1511	Event-ID
Authentication	Category
SGAuthentication	Source
Logon user ’Administrator’	Description of the event

29.7 Notes

- If a log file is to be stored on an external medium like a removable disk, an error message is written to the event viewer if the disk space is exceeded.

  We recommend that you avoid logging to an external medium.

- Events that cannot be written to a log file are stored in the event viewer.

- If several workstations want to write to a defined log file at the same time (e.g. a file that is being shared over the network), problems may occur. To avoid data being lost, Auditing offers the following solution: if a log file is inaccessible because it is being used by another workstation, Auditing creates new log files to which the workstations that could not access the original file can write their events.

  The new log files have the following structure:
  Access denied for log file Sglog.txt > log file Sglog.txt.1 is created
  Access denied for log file Sglog.txt and Sglog.txt.1 > log file Sglog.txt.2 is created
  etc.

  A maximum of 999 files can be created. If the file number exceeds 999 the events are automatically logged to the event viewer. This procedure is applied if the log file is in read-only mode or if it exceeds 2 GB. The log file created by SGE has to be explicitly deleted when uninstalling the product.

  We recommend that you avoid logging several workstations in the same log file and use remote logging to log several workstations.

- **SNMP traps**
  You can generate SNMP traps from Auditing if something happens on a client machine which needs to be reported to the Administrator.

  A Utimaco solution description gives details of how to use SNMP and Auditing.

  You will find more information on this subject in the Utimaco Knowledge Database **http://www.utimaco.com/myutimaco**.

  Use the Knowledge database's "Search" field to look for key words like "SNMP".

30 Central administration

In addition to previous management mechanisms, there is a specific application that performs centrally-administered tasks. It administers all installed SafeGuard Easy clients in a corporate network and also ensures the secure central distribution of configuration data to groups of clients, displays their current status, and acts as a central archive for system kernel backups. Even clients that are not regularly connected to the network (offline clients) can be integrated into central administration.

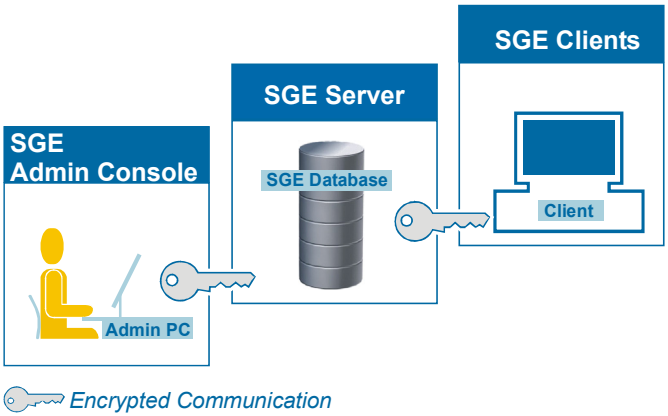
The administration mechanism used in previous versions (using the configuration file and software tools from third-party suppliers) can still be implemented.

30.1 Functionality

In centralized administration, SafeGuard Easy client PCs can be controlled from one central point via the Administration Console. The Administration Console manages a central database which contains the configuration settings for the SafeGuard Easy clients. In addition, any other data, such as any changes to these configuration settings, can also be stored in this database.

The SafeGuard Easy central administration system uses the following components:

- The SafeGuard Easy server with the SafeGuard Easy database.
- The SafeGuard Easy Administration Console which controls the Database on the Server.
- SafeGuard Easy client PCs



The central SafeGuard Easy Database collects different information about the SafeGuard Easy Clients. The SafeGuard Easy administrator uses the Administration Console to manage the contents of the database and to create any requests for change, referred to simply as "requests".

The SafeGuard Easy clients use a network agent to load the configuration changes from the database via the server and report successful changes back to the server. If the change is successful, the server then stores the new configuration settings in the database. Communication with the SafeGuard Easy server is set up via the SafeGuard Easy server process which uses an ODBC interface to guarantee maximum flexibility in selecting which type of database should be used.

30.1.1 SafeGuard Easy Server/ SafeGuard Easy Database

The SafeGuard Easy Server is the central storage location for all clients, as the settings for all SafeGuard Easy clients are saved on it in one database. SafeGuard Easy can use any database that implements an OBDC interface. The default database in SafeGuard Easy is Microsoft Access.

The SafeGuard Easy Database on the SafeGuard Easy Server contains the following information about the SafeGuard Easy clients:

- Current SafeGuard Easy settings (except their passwords and keys)
- Network name

You can use the SafeGuard Easy Administration Console to view this information.

On the Server, SafeGuard Easy also creates the Backups folder, in which a system kernel backup is automatically created for each workstation registered on the Server. This backup is updated after any configuration changes.

NOTE:
If you plan to operate SafeGuard Easy together with the server-based administration in a new installation, you might prefer to deploy Utimaco's next-generation product SafeGuard Enterprise from the start. SafeGuard Enterprise provides enhanced management options including Active Directory integration, web service based policy distribution, as well as Windows Vista support. For further information simply contact your local SafeGuard Easy sales partner.

NOTE:

Naturally, there may be several SafeGuard Easy Servers on the network, for technical or organizational reasons, to which the SafeGuard Easy Clients can be assigned. Version 4.50 of SafeGuard Easy provides **no** support for synchronization between servers. This functionality may be supplied by a database with replication tools.

30.1.2 SafeGuard Easy Administration Console

The Administration Console is a program that accesses the Server Database and, for example, triggers the central distribution of configuration files. Only privileged users are permitted to access the Administration Console.

These are some typical tasks taken on by the Administration Console:

- querying the settings of SafeGuard Easy clients and defining their status (Offline, Standard, Push).
- grouping the SafeGuard Easy clients to simplify administration.
- generating new configurations which are then distributed to the SafeGuard Easy clients.
- monitoring the correct processing of the distributed configuration files.

The Administration Console does not have to run on the same machine as the SafeGuard Easy Server, but can be installed and accessed on every computer on the network. Only the name of the SafeGuard Easy Server computer needs to be known, and a network link is required.

To ensure data consistency, **only one administrative connection** is possible at once. Attempts to create several admin connections simply fail.

30.1.3 SafeGuard Easy Clients

SafeGuard Easy Clients with an installed network agent ("Server connection" option) are able to establish a link with the SafeGuard Easy Server. The link between the SafeGuard Easy Server and SafeGuard Easy Client is created via a network agent and the UNC NetBIOS "name of the SGE Server", which is passed on to each client during installation.

When it is initially registered on the SafeGuard Easy Server, the SafeGuard Easy Client reports to following information:

- its SafeGuard Easy configuration settings
- the GUID
- its public key
- its network name.

In addition, when it is initially registered, it also exchanges public key with the Server.

Whenever the SafeGuard Easy Client contacts the Server, in the future, it queries the Server to obtain updates for any relevant settings. Usually the SafeGuard Easy Clients attempt to create a link to the SafeGuard Easy Server each time the PC boots. During this phase, all changes stored centrally on the SafeGuard Easy Server are gathered, fetched, and executed on the client.

If changes are made locally on the SafeGuard Easy Client (if, for example, the Administrator changes settings on site), the Client reports them to the Server immediately, to keep the database up-to-date. If there is a uninstallation, the Client reports this uninstallation to the Server, which deletes the entry for the Client concerned from the database.

30.1.4 Supported SafeGuard Easy Client-/ SafeGuard Easy Server combinations

SafeGuard Easy Client and SafeGuard Easy Server versions are generally compatible with older versions. For example SafeGuard Easy Server V4.50 works with SafeGuard Easy Clients, V4.40, without any problems, and vice versa.

For SafeGuard Easy Clients < V4.11 there are some restrictions:

- Changing SafeGuard Easy Client status to .OFFLINE not possible
- Re-registering a SafeGuard Easy Client not possible
- Registering SafeGuard Easy Clients to another SafeGuard Easy Server not possible

30.2 Exchanging Data between Client and Server

In the current version of SafeGuard Easy, sensitive SafeGuard Easy information is no longer just transferred using configuration files, but also exchanged online between the SafeGuard Easy Server and SafeGuard Easy Client. This link needs to be protected and configured.

30.2.1 Secure communication

The data transfer is encrypted to ensure the SafeGuard Easy information is properly protected. However, it is only sensible to encrypt the link after each client has authenticated itself on the SafeGuard Easy Server, for information exchange, and vice versa.

> ***NOTE:***
> The Client and Server communicate over Microsoft's RPC/DCOM service. The communication ports/protocols are freely selectable.
> If you are using a firewall, open the communication ports for the Client and Server. For details about RPC/DCOM read the relevant Microsoft documentation.

Client/Server authentication

SafeGuard Easy uses strong encryption with public/private key procedures for mutual authentication. The RSA procedure, with a 1024-bit key length, is used to generate the key pair. The communication between Client and Server is protected by the Interlock protocol.

If no RSA key pair is available it is generated on the client/server while the SafeGuard Easy software is being installed. Once the keys in the pair have been generated, they are stored, unchanged, on the PC.

When the Server and Client make contact, they exchange public keys and check each other's authenticity for the first time. Both the Client and the Server save the public key and "know" each other from this point in time.

Next time the Client and Server communicate with each other, they use the exchanged public key to verify each other's private key and check each other's identity.

Optionally, a Trusted Platform Module such as the Lenovo ESS chip can also be given the task of generating the key pair. This procedure ensures additional hardware security for the key memory, but is slower than the software-based solution.

Data encryption during the transfer

All SafeGuard Easy information that passes to and from the SafeGuard Easy Server is encrypted. After successful mutual machine authentication a random symmetrical session key is generated, exchanged, and used for encrypted data transfer during the time that the link exists.

A new random key is used for each session for each connection between SafeGuard Easy client and SafeGuard Easy Server. The same procedure is used for communication between the SafeGuard Easy Administration Console and SafeGuard Easy Server.

RC4, with a 128-bit session key, is used to perform encryption.
The session key can be created by the Client or the Server and will be encrypted with the public key of the recipient before it is sent.

30.2.2 Expected network load

The amount of data generated when the SafeGuard Easy client checks for configuration updates when it is being booted is only slightly different from the amount of data generated when it checks for configuration updates after a specified defined time period, and depends on whether there are changes, and which ones there are. In both cases around 2 Kbytes of data are exchanged. The exact amount depends to some extent on many changes there are.

If you already use configuration files to install/configure SafeGuard Easy, the size of these files gives you an approximate idea of the amount of data involved.

Due to the fact that you can configure the data exchange interval, as described in 'Maximum capacity of the SafeGuard Easy Database', it is the view of Utimaco that central SafeGuard Easy Administration makes a negligible contribution to increased network load.

30.2.3 Defining the interval for data exchange

Usually a Client checks with the Server when it is being booted, to find out whether changes are to be made. It checks again at pre-defined intervals. **The default value** for additional update checks is **6 hours**.

You can customize this interval centrally, using standard Windows mechanisms, as it is a Windows Registry entry. To adjust the interval, re-generate the [DWORD] registry key:

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy

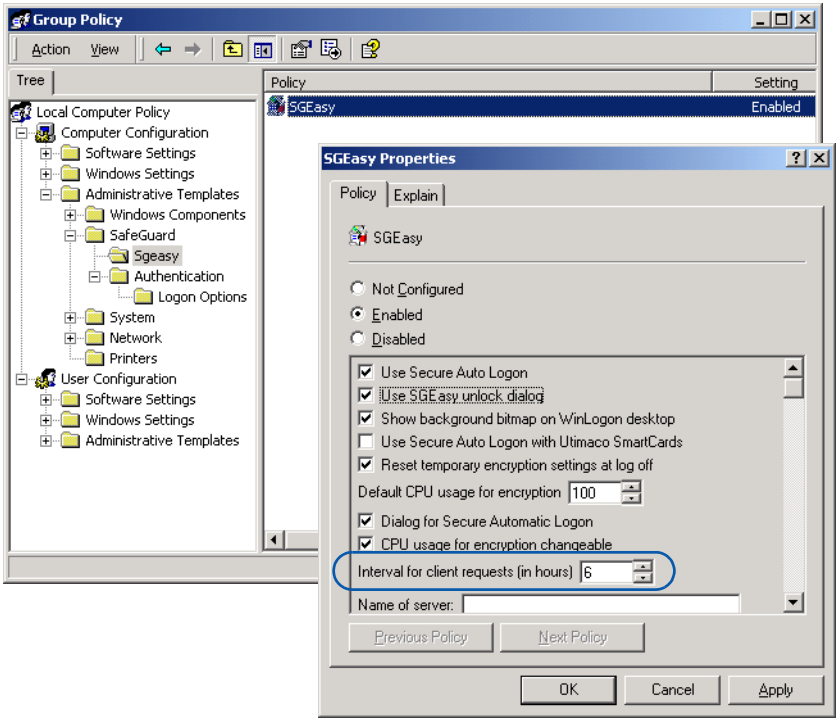
"**NotifyPeriod**"=<interval>

If this registry key is present, clients check for requests at the specified intervals. You can enter values between 1 and x hours.

You can also modify the interval via a policy in Utimaco's administrative template. You will find the policy in

Computer Configuration
\Administrative Templates
\SafeGuard
\SGEasy

On the “SGEasy“ property page enter a value for the “Interval for client requests“.



30.3 Installation

Note about Windows XP SP 2/Windows Server 2003 SP 1
If you use the optional central administration server or SafeGuard Easy 4.x Remote Administration you must make a few special configuration settings in Windows XP in SP2 and Windows Server 2003 SP 1.

You will find a description of all the necessary settings in our Knowledge Database **http://www.utimaco.com/myutimaco** in **Knowledge Item "106898 SafeGuard Easy and SP2 Configuration for Windows XP"**. Use the Knowledge database's "Search" field to look for "106898".

In the CD's \Tools directory you will also find a tool for automatically setting the necessary properties to use central administration and remote administration.

Requirements

- **Microsoft High Encryption Package**
  The prerequisite for central administration is that the operating systems on the Client, Server and the PC with the Administration Console support encryption with 128-bit keys. In addition, the Microsoft "**High Encryption Package**" must be installed on all machines involved. You can find out whether it is installed via Internet Explorer (Help/About Internet Explorer/Cipher Strength menu option).

  The high encryption package is installed by default in Windows XP and in Windows 2000 from Service Pack 2 (or higher).

- **Ports**
  The Client and Server communicate over Microsoft's RPC/DCOM service. The communication ports/protocols are freely selectable. If you are using a firewall, open the communication ports for the Client and Server.

  For details about RPC/DCOM read the relevant Microsoft documentation.

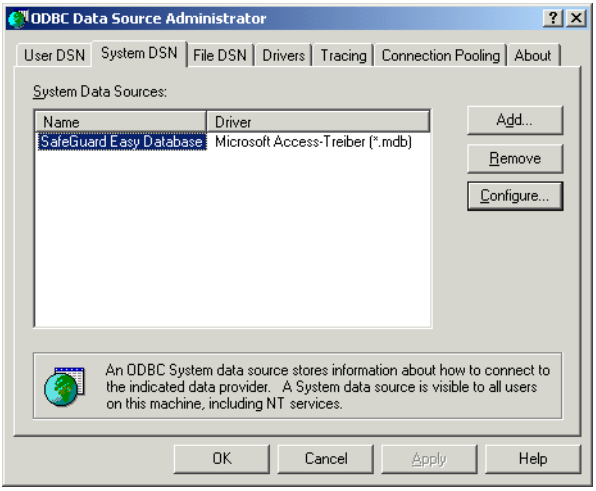
30.3.1 Installing SafeGuard Easy Server/Database

The computer on which the SafeGuard Easy Database is installed is the "core" of central administration and should be the first to be created, or at least you should know the computer's name so that you can pass it on to the SafeGuard Easy clients.

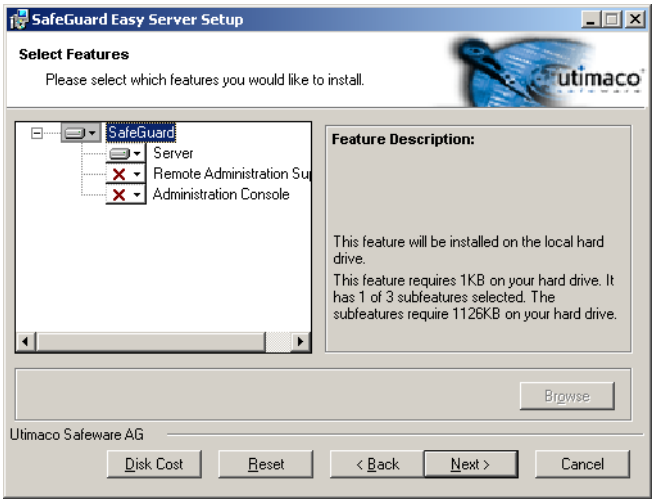
We recommend that you do not change the workstation name of the SafeGuard Easy Server after registering the clients. This would mean that communication between Clients and the Server would be interrupted and no more data exchange could take place!

The SafeGuard Easy Server can be located on a physical network server or on any workstation on the network. The prerequisite for connecting a client to the central SafeGuard Easy Database is that a suitable network protocol is installed on all workstations, and active.

When you install the Server component, no application is installed. Instead a Microsoft Access database (Sgeasy.mdb) is simply generated in the SafeGuard Easy Installation folder on the Server (see Settings/Control Panel/Administrative Tools/Data Sources (ODBC)). This database is password-protected.



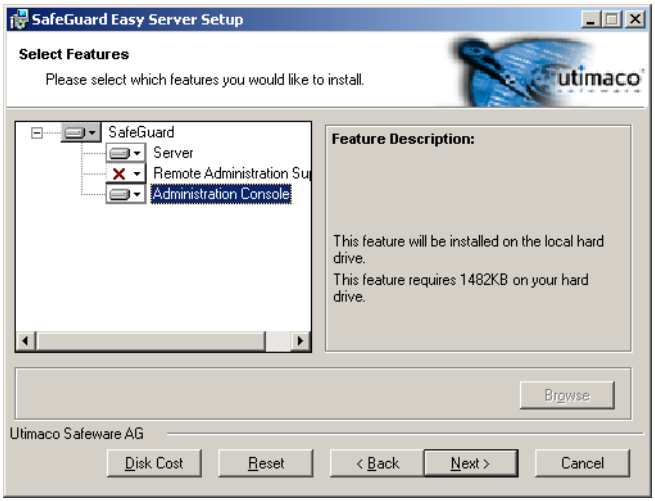
To install the SafeGuard Easy Server, run `Server.msi` in the **..\SERVER** folder on the CD. In a "Custom" installation, select the "Server" option. When you have finished installation, you will need to restart your system.


SafeGuard Easy Server Setup
Select Features
Please select which features you would like to install.
utimaco
SafeGuard
Server
Remote Administration Su
Administration Console
Feature Description:
This feature will be installed on the local hard drive.
This feature requires 1KB on your hard drive. It has 1 of 3 subfeatures selected. The subfeatures require 1126KB on your hard drive.
Browse
Utimaco Safeware AG
Disk Cost
Reset
< Back
Next >
Cancel

30.3.2 Installing SafeGuard Easy's Administration Console

Generally it is not desirable to carry out installation and configuration directly on the server. For this reason, the database should be administered from an admin workstation. You can use any workstation as an admin workstation, provided it has a network link to the Server machine.

To install the Administration Console, run `Server.msi` in the ...\SERVER folder on the CD. In a "Custom" installation, select the "Administration Console" option, and start installation.



When you have finished installation, you will need to restart your system.

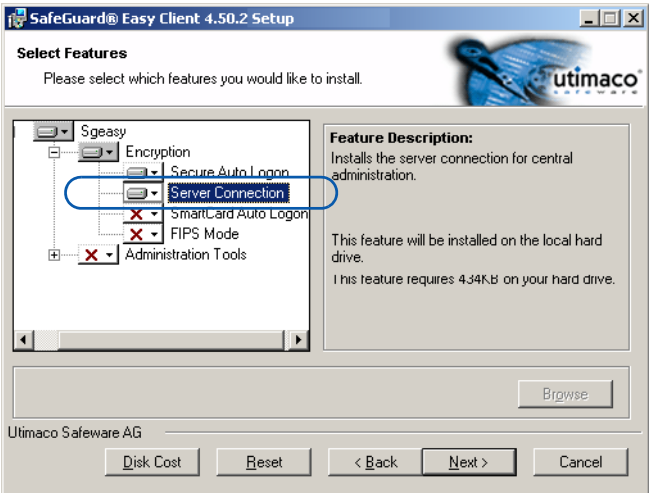
After you have restarted your system, you will find the entries Administration Console and Configuration File Wizard in Programs/ Utimaco/SafeGuard Easy.

30.3.3 Installing SafeGuard Easy Clients

The installation procedure proceeds in the usual way (see Local or Central Installation). However, for communication with the Server, the clients need to be told the UNC NetBIOS name of the SafeGuard Easy Server and of the "network agent" that enables communication with the Server.

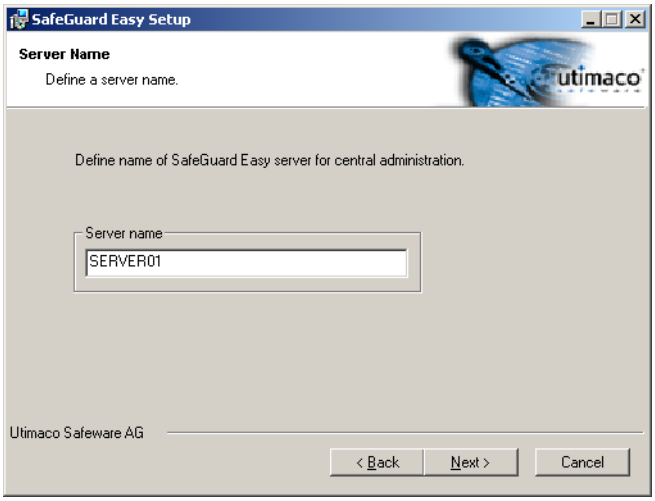
You cannot tell them the name of the network agent after you have installed SafeGuard Easy! If you want a Client to be administered centrally, you must re-install SafeGuard Easy with an activated network agent.

To start installation, run `Sgeasy.msi` in the ...\CLIENT folder on the CD (interactive installation). In a "Custom" installation, select the "Server Connection" option, along with the already-selected components.



Later, in the course of installation, you enter the name of the SafeGuard Easy Server (for example, "SERVER01") in the *Server* dialog.

To handle an "Offline client", this client must be issued a specially reserved "server name" (".OFFLINE") which activates an alternative communication mechanism. For details regarding offline clients see 'State "Offline"'.



Continue installation as described in "Local Installation". When you have finished installation, you will need to restart your system.

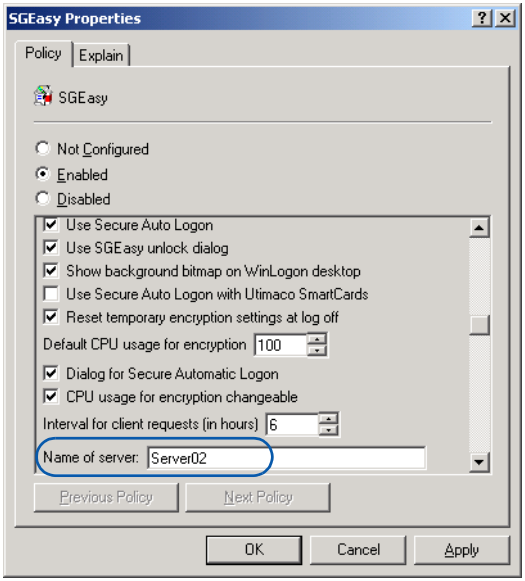
WARNING:
If the name of the SafeGuard Easy client is changed after SafeGuard Easy is installed, the Server will no longer recognize the Client. As a consequence the SafeGuard Easy Client entry will have to be deleted from the database and SafeGuard Easy will have to be re-installed on the Client. After re-installation the Client registers itself with a new name.

Supplying a SafeGuard Easy client with the SafeGuard Easy server name after installation

If you currently do not know the server name you can leave the Server Name field empty for the moment. The server name can be added centrally on the client using standard Windows mechanisms because it is simply an entry (‘Name of Server‘) in Utimaco’s administrative template.

You will find the policy in the administrative template at

Computer Configuration
\Administrative Templates
 \SafeGuard
  \SGEasy



30.3.4 Maximum capacity of the SafeGuard Easy Database

The SafeGuard Easy database is, by default, a Microsoft Access database. The maximum size of any Microsoft Access database is 2 GB, but it can be extended by links to other databases.

After registration, a SafeGuard Easy Client needs approximately 5 to 7 KB of the database's memory. For 50,000 clients this means around 340 to 350 MB.

However, we recommend that you do not use one (server) database to administer such a large number of workstations. You should instead implement a suitable organizational and administrative structure in which the workstations are administered via a number of servers.

30.3.5 Restoring a SafeGuard Easy Server or Database

To successfully restore a SafeGuard Easy Server you should:

- Save these specific files, which are usually located in the product directory (C:\Programs\Utimaco\SafeGuard Easy):
  - Sgeasy.mdb
  - WksInfo.stg
  - Pubkey.sto
- Write down the NetBIOS name and IP address of the (old) SafeGuard Easy Server for the purpose of restoration.

Using the saved files, NetBIOS name and IP address you can restore the last backup of the files when you set up a SafeGuard Easy Server again.

Here, please note the following points:

1. Ensure you assign the new PC (server) the same IP address and the same NetBIOS name.
2. Now re-install the SafeGuard Easy Server (Server.msi).
3. After the installation is complete, *do not* restart the PC immediately.
4. Load the three saved SafeGuard Easy files into SafeGuard Easy's product directory.
5. Restart the PC.
6. After the restart, open SafeGuard Easy's Administration Console. The SafeGuard Easy client's entries are now present.

30.4 Microsoft SQL Server support

SafeGuard Easy uses a Microsoft Access database as the default database type for saving information about SafeGuard Easy clients. Some users would perhaps prefer to use a different database type. To meet this customer requirement, SafeGuard Easy has extended the range of supported databases by adding Microsoft SQL Server.

There are two phases in setting up Microsoft SQL Server support:

- Firstly an empty SafeGuard Easy database must be generated on the SQL Server.
- Then, this empty database must be registered on the SafeGuard Easy Server.

30.4.1 Important information

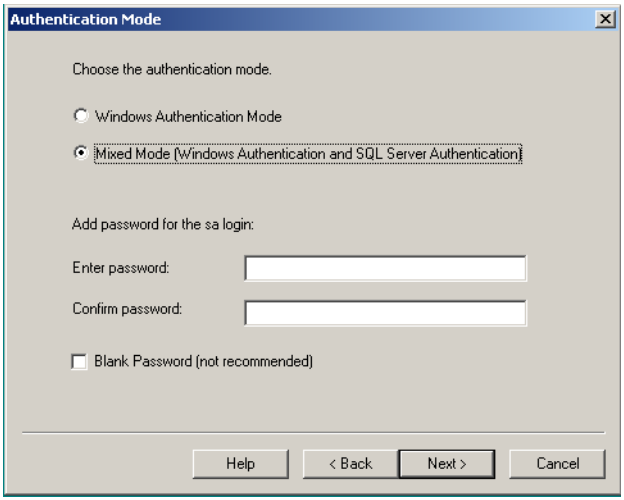
- Microsoft SQL Server is only supported from SafeGuard Easy 4.11 onwards.
- Microsoft SQL Server can, but need not, be installed on the machine on which the SafeGuard Easy Server is later installed.
- If you plan to use a database then you should not instal or register any SafeGuard Easy clients until you have set Microsoft SQL Server as the default database.
- SafeGuard support for SQL Server has been developed and tested with the following versions:
  - SQL Server 2005
  - SQL Server Enterprise Edition 8.00.760 (ServicePack3)
  - SQL Server Developer Edition 8.00.194 (RTM)

30.4.2 Generating an empty SafeGuard Easy database on the SQL Server

NOTE:
You must do this BEFORE installing the SafeGuard Easy Server!

1. Install SQL Server (if not already present).

   During installation, note these points:
   As Authentication Mode select the option "Mixed Mode".



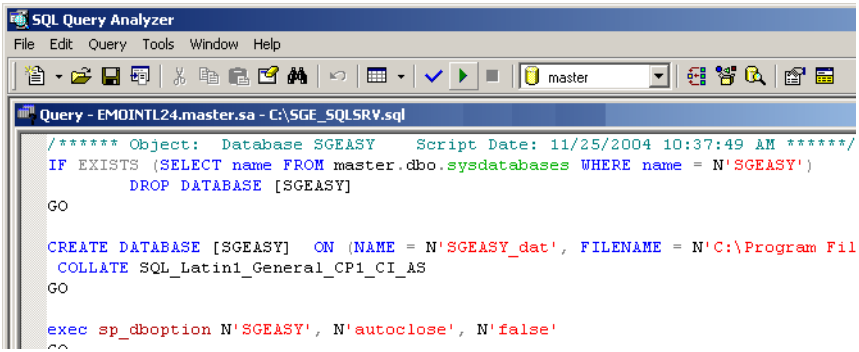
   You can also change the Authentication Mode after installing SQL Server.

2. Run SQL Query Analyzer by selecting **Programs/Microsoft SQL Server/Query Analyzer**.

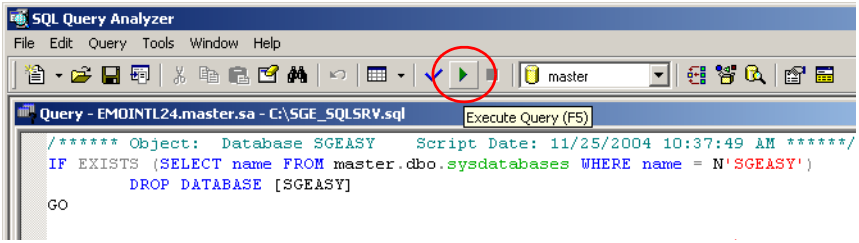
3. Open the `SGE_SQLSRV.sql` file in the Query Analyzer. ((You will find the file in the `SQL-info.zip` file in the \TOOLS folder on the SafeGuard Easy CD).

   `SGE_SQLSRV.sql` contains the script that is needed to generate an empty SafeGuard Easy Database on the SafeGuard Easy Server. This database is later used as a SafeGuard Easy Database by SafeGuard Easy Server.

   Overwrite the entry "C:\program files\Microsoft SQL Server" with the installation folder of the SQL Server on your PC (for example. "D:\Microsoft SQL Server").

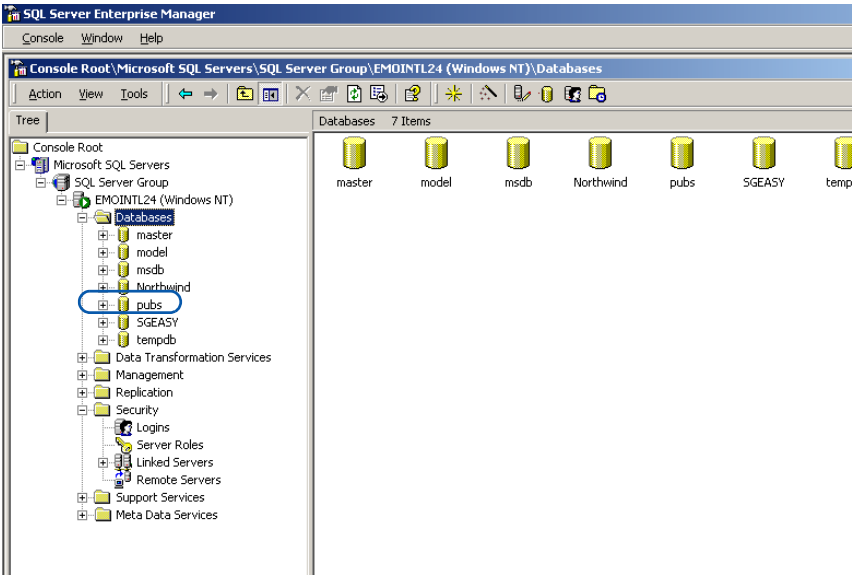

SQL Query Analyzer
File Edit Query Tools Window Help
master
Query - EMOINTL24.master.sa - C:\SGE_SQLSRV.sql
/****** Object: Database SGEASY Script Date: 11/25/2004 10:37:49 AM ******/
IF EXISTS (SELECT name FROM master.dbo.sysdatabases WHERE name = N'SGEASY')
DROP DATABASE [SGEASY]
GO
CREATE DATABASE [SGEASY] ON (NAME = N'SGEASY_dat', FILENAME = N'C:\Program Fil
COLLATE SQL_Latin1_General_CP1_CI_AS
GO
exec sp_dboption N'SGEASY', N'autoclose', N'false'

4. Run the SGE_SQLSRV.sql - script.

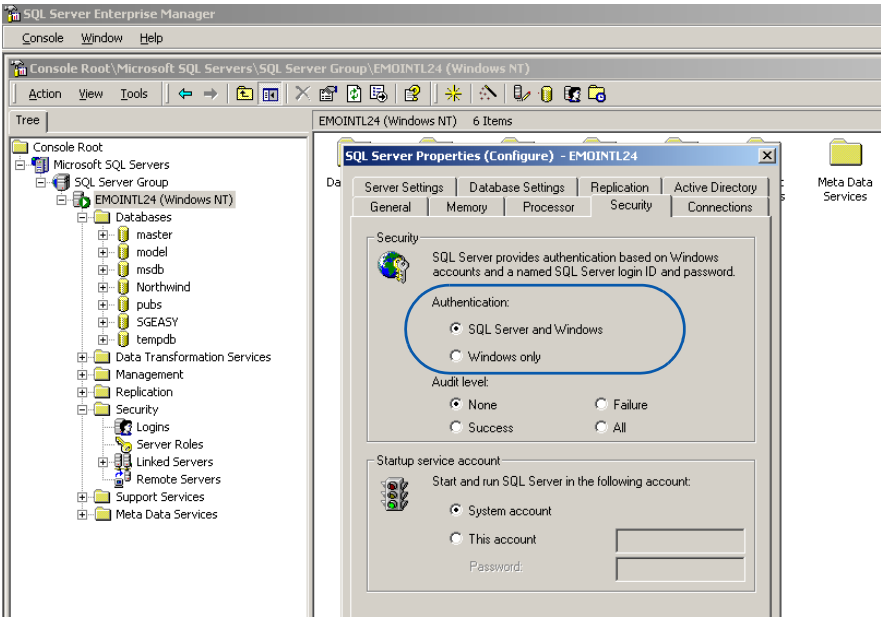

SQL Query Analyzer
File Edit Query Tools Window Help
master
Query - EMOINTL24.master.sa - C:\SGE_SQLSRV.sql
Execute Query (F5)
/****** Object: Database SGEASY Script Date: 11/25/2004 10:37:49 AM ******/
IF EXISTS (SELECT name FROM master.dbo.sysdatabases WHERE name = N'SGEASY')
DROP DATABASE [SGEASY]
GO

5. After you have run the script, call the Enterprise Manager by selecting **Programs/Microsoft SQL Server/Enterprise Manager**.

6. An empty SafeGuard Easy database with the name "SGEASY" has been generated in your SQL Server.



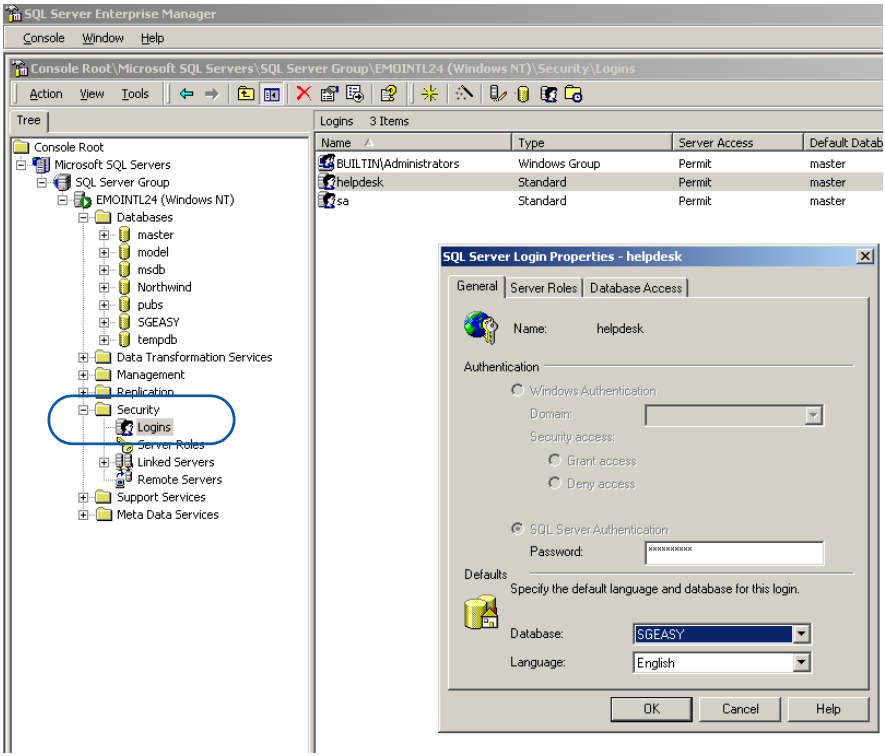
7. If this has not already happened during the SQL Server installation, then select your own SQL Server in the tree structure (in our example, EMOINTL24 (Windows NT) and then display the Properties page in the context menu.



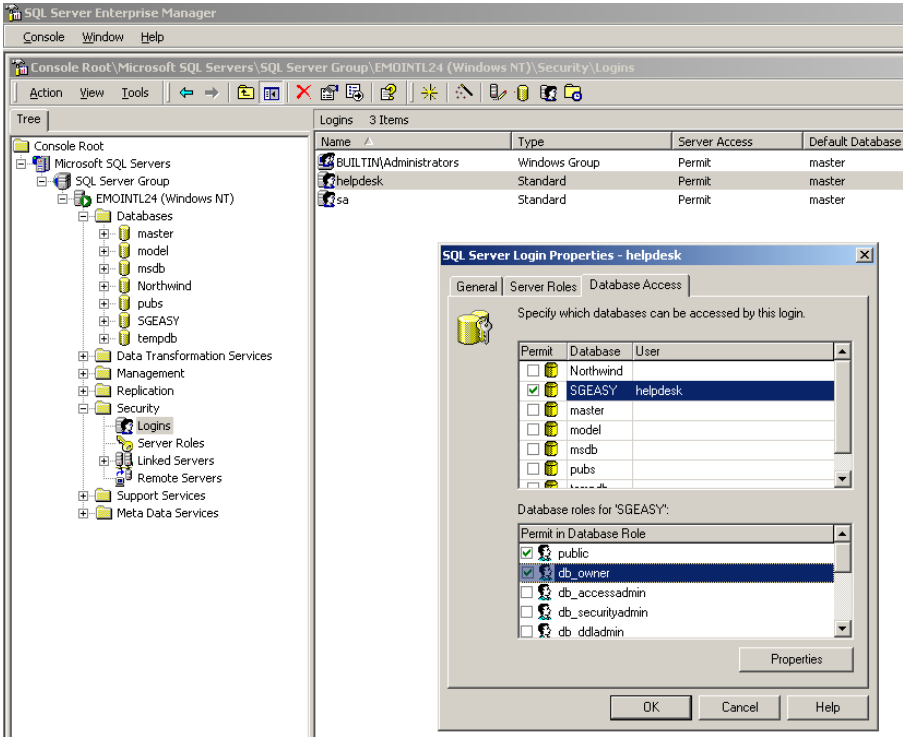
In the "Security" tab set the authentication to "SQL Server and Windows".

8. Optionally: a system account other than the standard one (the default is user "sa") for the SGEASY database can be generated via Security > Logins > context menu "New Login".

   In the "General" tab under "Authentication" select the "SQL Server Authentication" option and enter the Password. Set SGEASY as the "database".



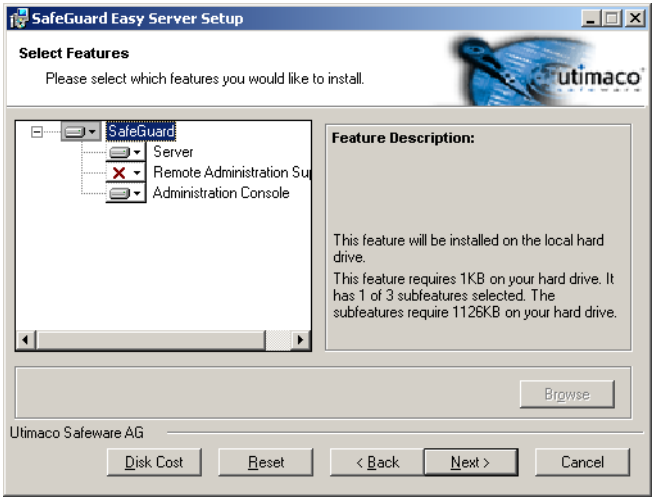
In the "Database access" mark "public" and "owner" as permitted roles.



30.4.3 Registering the new (empty) SafeGuard Easy Database on the SafeGuard Easy Server

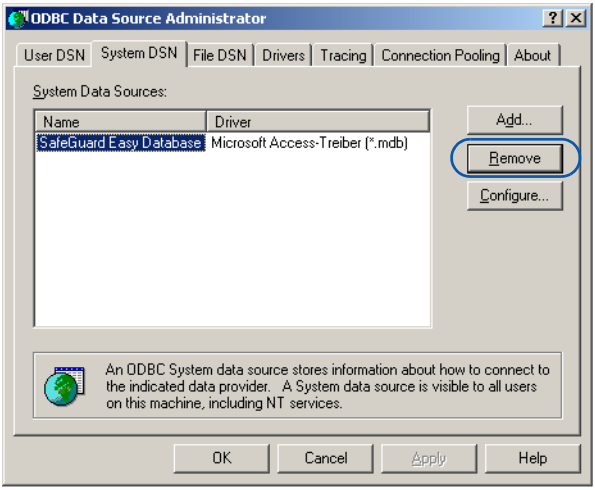
1. Install SafeGuard Easy Server by opening the `Server.msi` file in the \SERVER folder on the product CD. If required, you can also install the Administration Console, as well as the Server.

> ***WARNING:***
> Do NOT reboot the PC after SafeGuard Easy Server installation!

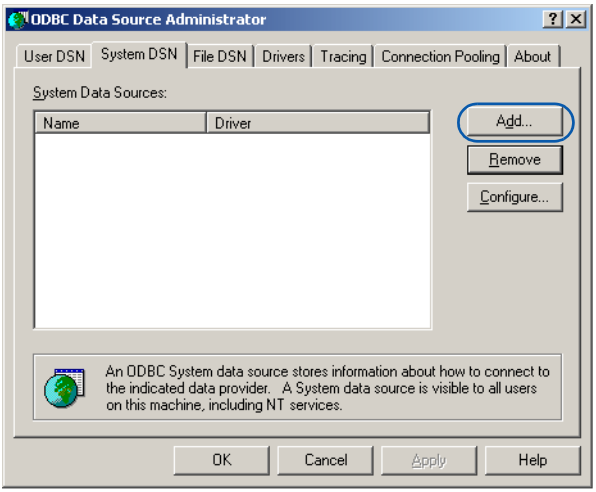

SafeGuard Easy Server Setup
Select Features
Please select which features you would like to install.
utimaco
SafeGuard
Server
Remote Administration Su
Administration Console
Feature Description:
This feature will be installed on the local hard drive.
This feature requires 1KB on your hard drive. It has 1 of 3 subfeatures selected. The subfeatures require 1126KB on your hard drive.
Browse
Utimaco Safeware AG
Disk Cost
Reset
< Back
Next >
Cancel

2. Select **Settings/Control Panel/Administration/Data sources (OBDC)**.

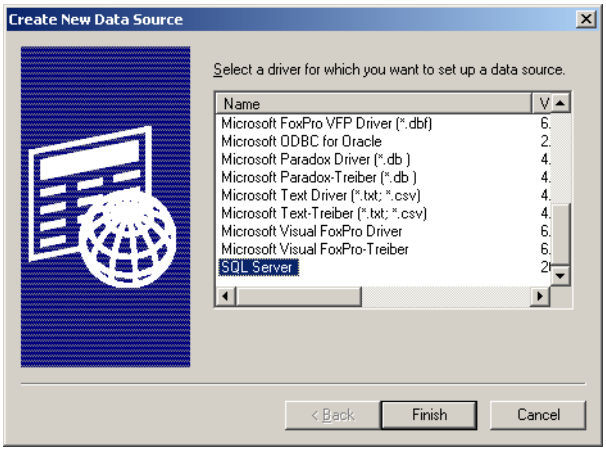
3. Open the "System DSN" tab and remove the default "SafeGuard Easy Database" with the Microsoft Access driver from the list..



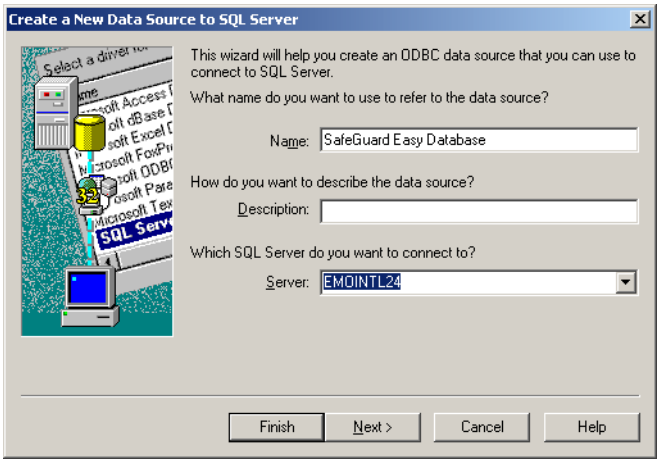
4. To create a new data source click [Add...] in the System DSN tab.



5. Select "SQL Server" as the driver for the new data source.

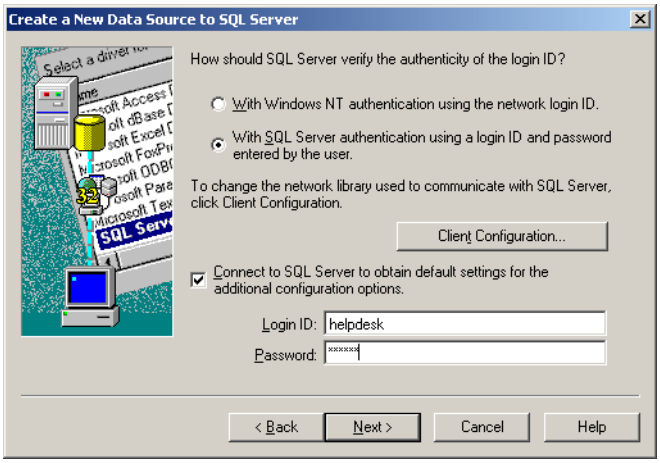


6. Create the connection to the SQL Server.

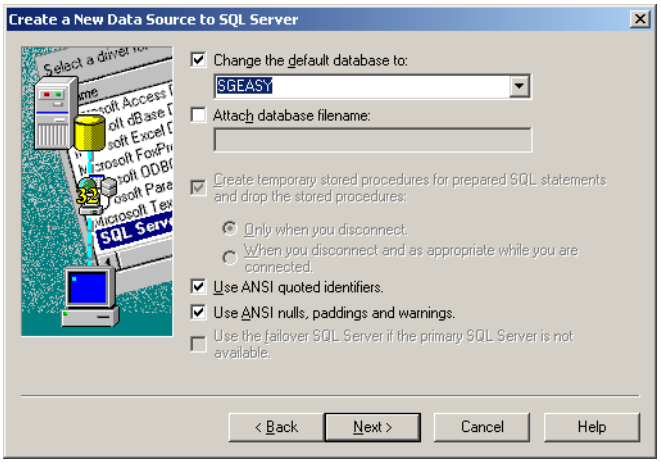

Create a New Data Source to SQL Server
This wizard will help you create an ODBC data source that you can use to connect to SQL Server.
What name do you want to use to refer to the data source?
Name:
SafeGuard Easy Database
How do you want to describe the data source?
Description:
Which SQL Server do you want to connect to?
Server:
EMOINTL24
Finish
Next >
Cancel
Help

NOTE:
The name of the database MUST BE "SafeGuard Easy Database"!

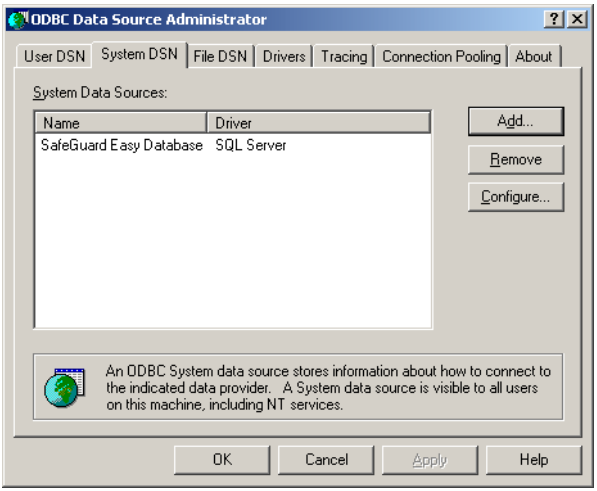
7. Select the "With SQL Server authentication ..." option and select the default user for the SQL database (usually user "sa" or, in the example user "helpdesk").


Create a New Data Source to SQL Server
How should SQL Server verify the authenticity of the login ID?
With Windows NT authentication using the network login ID.
With SQL Server authentication using a login ID and password entered by the user.
To change the network library used to communicate with SQL Server, click Client Configuration.
Client Configuration...
Connect to SQL Server to obtain default settings for the additional configuration options.
Login ID:
helpdesk
Password:
< Back
Next >
Cancel
Help

8. Select "SGEASY" as the default database and keep the other default settings.


Create a New Data Source to SQL Server
Change the default database to:
SGEASY
Attach database filename:
Create temporary stored procedures for prepared SQL statements and drop the stored procedures:
Only when you disconnect.
When you disconnect and as appropriate while you are connected.
Use ANSI quoted identifiers.
Use ANSI nulls, paddings and warnings.
Use the failover SQL Server if the primary SQL Server is not available.
< Back
Next >
Cancel
Help

9. The SQL database now appears as the "new" SafeGuard Easy database type.

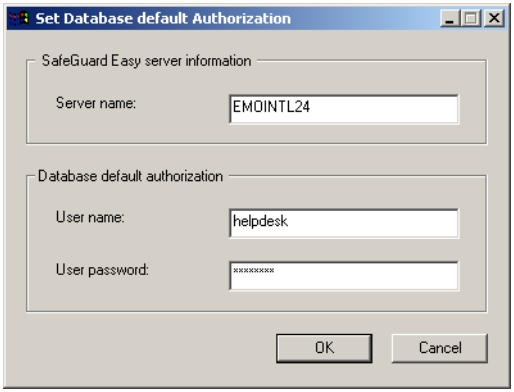


10. Restart the system and stop SGEasy's SgeSrv.exe and CfgDBSrv.exe services (SafeGuard Easy Server=SgeSrv.exe and SafeGuard Easy Database Server=CfgDBSrv.exe).

11. The access data for the SafeGuard Easy database is not transmitted in plain text. The `SetDBPwd.exe` tool updates the default user and stores the password in the encrypted file `DBPwd.stg` so that it can be used by the SafeGuard Easy Server.

> ***NOTE:***
> Step 10 and 11 are NOT necessary if the default database user logs on WITHOUT a password!

You should run the `SetDBPwd.exe` file (located in your SafeGuard Easy Server installation directory) and enter the data for which you are prompted.



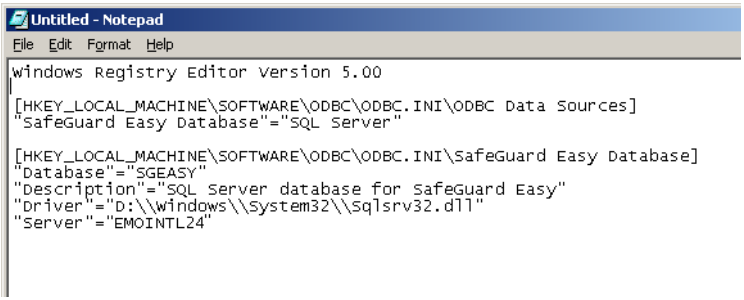
NOTES:

- The name of the PC (or the IP address) on which the SafeGuard Easy Server is installed must appear in the "Server name" field, (in the example the SafeGuard Easy Server and SQL Server are installed on the same machine).
- The user data for the SGEASY database on the SQL Server must be entered under "Database default authorization"!
  If a user account that is not the default user (in our example, "helpdesk") wants to log on, it must be available to the SGEASY database and have the appropriate rights.

12. Reboot the PC.

Users can replace steps 4 to 7 in this way:

1. Open the Registry file `SGE_SQLSRV.reg`. (You will find the file in the SQL-info.zip file in the \TOOLS folder on the SafeGuard Easy CD).



2. Change the following keys:

   - **"Driver"**
     Enter the correct path for the `SQLSRV32.dll` file on your SafeGuard Easy Server (for example "D:\\Windows\\System32\\SQLSRV32.dll")
   - **"Server"**
     Enter the name of the SQL server (e.g. "EMOINTL24").

3. Run `SGE_SQLSRV.reg`.

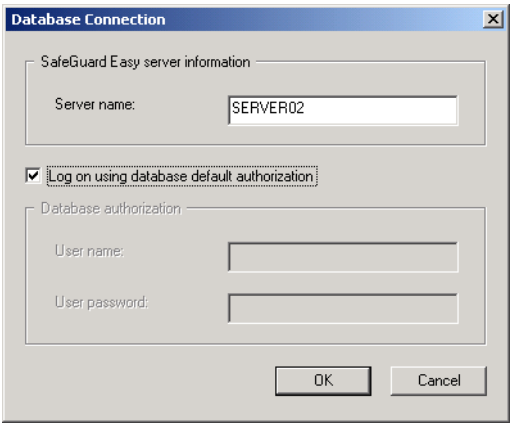
31 Administration Console

Before the full functionality of the Administration Console can be used, a link needs to be established to the SafeGuard Easy Server.
The SafeGuard Easy Server holds the SafeGuard Easy Database, its OBDC registration and the Server process.

31.1 Logging on to the Administration Console

To start the Administration Console, select **Start/Programs/Utimaco/ SafeGuard Easy/Administration Console**.

You see a logon screen.



In the logon screen, enter the following information:

- **Server name**
  Name of the SafeGuard Easy Server on which the SafeGuard Easy Database is held. You can also enter an IP address to identify the server.

- **Access data for database**
  If "Log on using database default authorization" is selected, SafeGuard Easy uses the current default logon data for the SafeGuard Easy Database.

  The default setting is that the default user data is
  User name: Admin
  Password: *No Password*
  You can enter other access data if you deselect the selection check box.

After the link is successfully established, the server name and the user name (but not the database or the password) are saved in the Registry and automatically reused next time a user logs on. However, the Administration Console only links to the SafeGuard Easy Server automatically if the last logon was performed using the "default access data".

If you do not want to use the default data, simply close the link between the administration console and database by selecting the "Disconnect" command in the Administration Console's File menu. Then select the File menu "Connect" option to return to the database logon mask.

Usually the SafeGuard Easy Database and Administration Console are on the same machine (but this is not a prerequisite!).
If the SafeGuard Easy Database and the Administration Console are held on different machines (SafeGuard Easy Server and Administrator PC), the link is established via authentication using Windows user data, i.e. the user currently logged on to the Administrator PC must also use an appropriate user account to log onto the SafeGuard Easy Server.

31.1.1 Changing the access data for the database

You will find more information on this subject in the Utimaco Knowledge Database http://www.utimaco.com/myutimaco. Use the Knowledge database's "Search" field to look for key words like "Login & database".

The database supplied with SafeGuard Easy is a Microsoft Access database. During the installation of the SafeGuard Easy Server it is registered as an OBDC data source with the data source name (DSN) "SafeGuard Easy Database". The SafeGuard Easy Database uses the default OBDC driver for Microsoft Access, which is integrated in your Windows release. Since the OBDC driver for Microsoft Access is already installed as part of the base Windows 2000 and Windows XP functionality, it is not necessary to install Access to get access to the SafeGuard Easy database. If, however, for some reason, you want to change the default logon data for your database, Microsoft Access must be installed, so that you can create a user data file.

A Microsoft Access user data file contains information about users, passwords and group membership. By default, a user data file has the file extension .mdw and is also called a "Workgroup Information File" by Microsoft. A Microsoft Access installation generates the default Workgroup Information File `System.mdw` and stores it in

- MS Access 97 \WinNT\System32
- MS Access 2000 \Programs\Shared Files\System

You can use the MS Access tool `Wrkgadm.exe` to generate a new .mdw file and use it as a SafeGuard Easy user data file. However, you can also use the default .mdw file.

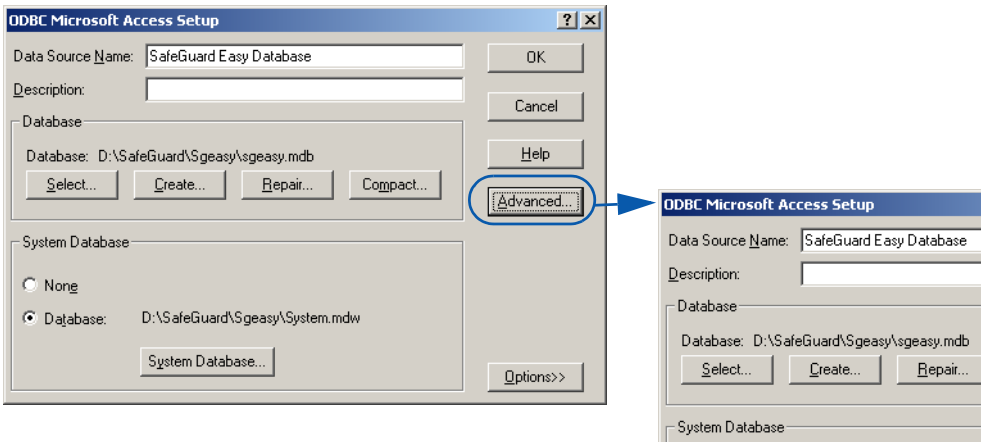
`Wrkgadm.exe` is stored at

- MS Access 97 \WinNT\System32\Wrkgadm.exe
- MS Access 2000 \Programs\Microsoft Office\Office\1033\

If you use the default .mdw file, you open MS Access. In the Tools/Security menu, select the "User and Group Accounts..." option. In the dialog you see next you can specify users, passwords and group memberships. Then, open Sgeasy.mdb, the SafeGuard Easy Database, with Microsoft Access. In the Tools/Security menu, select the "User and Group Permissions..." option. In the dialog you see next you can assign access rights to the specified users.

By default, SafeGuard Easy does not link the SafeGuard Easy Database with an .mdw file. In this case, the default logon data is the user name "Admin", without a password.

To allow other logon data to be used, select Programs/System Control/ Administration/Data Sources (OBDC)/System DSN/Configure. In the System Database field, enter the default .mdw file name `System.mdw`. If you click the "Advanced" button, you can also enter different default logon data. Please note that the user profile registered as the default also exists as an authorized user for the database.



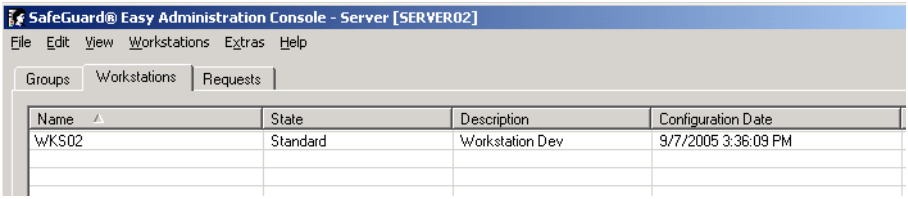
31.2 Admin Console user interface

When you successfully log on to the SafeGuard Easy Database, you see the Administration Console with the workstations, groups and requests tabs. To switch from one tab to another, simply click the appropriate tab or select the required item in the **View** menu.

Workstations

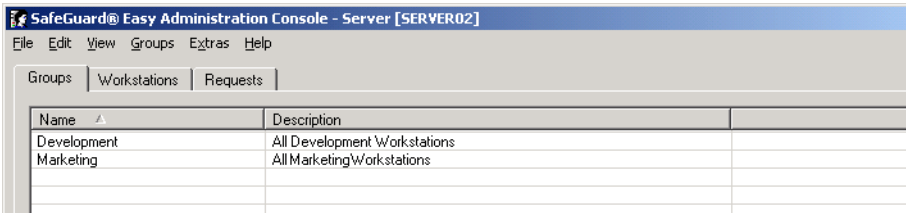
Displays a list of all SafeGuard Easy clients that have authenticated themselves on the Server.

- **Name:** the UNC NetBIOS name of each registered workstation.
- **State:** workstation is online (Standard) or offline
- **Description:** a more detailed description of the workstation.
- **Configuration Data:** a time stamp which tells when a SafeGuard Easy Client last finally sent its current configuration data to the SafeGuard Easy Server:


SafeGuard® Easy Administration Console - Server [SERVER02]
File Edit View Workstations Extras Help
Groups Workstations Requests
Name State Description Configuration Date
WKS02 Standard Workstation Dev 9/7/2005 3:36:09 PM

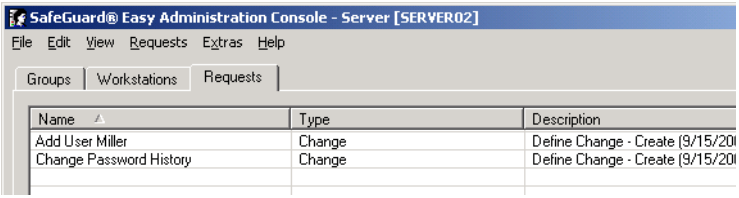
Groups

Displays a list of all created SafeGuard Easy groups in which individual SafeGuard Easy clients are gathered.

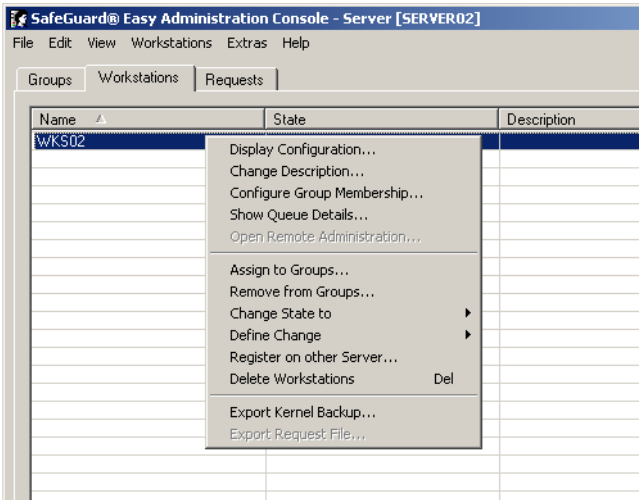

SafeGuard® Easy Administration Console - Server [SERVER02]
File Edit View Groups Extras Help
Groups Workstations Requests
Name Description
Development All Development Workstations
Marketing All MarketingWorkstations

Requests

Displays a list of all configuration changes that have been made, which have been, or will be carried out on SafeGuard Easy clients.


SafeGuard® Easy Administration Console - Server [SERVER02]
File Edit View Requests Extras Help
Groups Workstations Requests
Name Type Description
Add User Miller Change Define Change - Create (9/15/20
Change Password History Change Define Change - Create (9/15/20

You will also find the most important commands for a workstation, group or request in its context menu. In addition, you can call all these commands via the different menus (Workstations, Groups, Requests). The system displays the appropriate menus for the current tab (for example, if the Workstations tab is active, you see the Workstations menu, etc.).

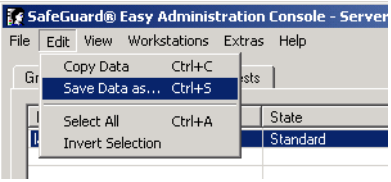


If several workstations, groups or requests are present, you can select several at once using standard Windows methods (Ctrl or Shift key and mouse-click, or via the **Edit** menu).

From the Administration Console you can also access **Remote Administration**, via the "Workstation/Remote Administration" menu option. For details of Automatic Logon, please read Chapter 'Remote Administration'.

31.2.1 Saving the contents of a tab as a text file

The Administration Console provides a function with which you can save the contents of the currently-active tab (Groups, Workstations or Requests) into a text file or "copy" it into the Clipboard. The text file and the clipboard contents can then be imported and processed in any program. This functionality becomes active as soon as a Group, Workstation or Request is selected. This method of saving the tab contents is particularly useful for archiving and evaluation purposes.



To call up the copy and save function, select **Edit Menu** in the Administration Console.

- The **Save Data as** menu item creates an ASCII file that can be saved to a directory with any name you choose. This file contains the column headers along with the selected tab entries.
- The **Copy Data** menu item "parks" the selected tab entries (without column headers) in the Clipboard. The Clipboard contents can then be inserted into any program you require.

31.3 Displaying the current configuration of a SafeGuard Easy Client

Once the SafeGuard Easy Client and SafeGuard Easy Server have successfully authenticated themselves, the user logged on to the Administration Console can view the client's SafeGuard Easy settings.

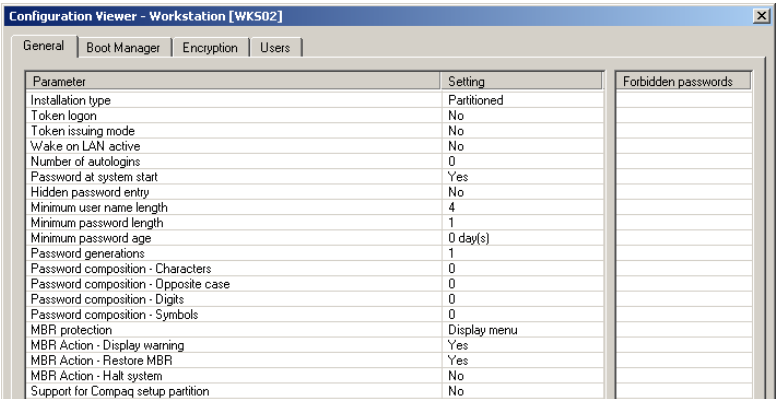
To check the current settings, or prepare for changes, we recommend that you always start by viewing the current configurations. In addition, you can use this function as an easy means to check whether requests have actually been successfully carried out on clients, or not.

To do this,

1. click the **Workstation** tab and select a SafeGuard Easy Client.

2. To view the details of the SafeGuard Easy settings, select the **Workstation/Current Configuration...** menu option.

3. You see a window with four tabs with the same names as in SafeGuard Easy Administration: General, Boot Manager, Encryption, and Users. Each tab shows the SafeGuard Easy configuration on the selected Client.



31.3.1 Changing a SafeGuard Easy Client description

You can give a new description to a workstation displayed in the "Workstation" tab by selecting the **Workstation** menu **Change description** option. The changed entries are applied immediately.

31.3.2 Removing a SafeGuard Easy Client

To remove a client from the list select the **Workstations/Delete request** menu option. The workstation will be deleted and removed from the list.

31.4 Re-registering a SafeGuard Easy Client

The mode for reregistering a SafeGuard Easy Client is needed if the SafeGuard Easy Client is not known to the SafeGuard Easy Server.

In practice, you might for example use this function in this scenario: in a company, the SafeGuard Easy Database is backed up each day at 5 am. At 8 am a new SafeGuard Easy Client successfully registers itself on the SafeGuard Easy Server and at 10 am the SafeGuard Easy Server crashes. The SafeGuard Easy Server is then recovered - but using the "old" database backup which was created at 5 am. This backup does not contain the new SafeGuard Easy Client that had registered itself at 8 am. The reregistering function is used to add the SafeGuard Easy Client to the SafeGuard Easy Database again.

For reregistering to succeed, the Administration Console user must know the valid SafeGuard Easy user data for the new SafeGuard Easy Client and use it to authenticate themselves on the Client.

> ***NOTE:***
> You can never reregister more than one Client at once!

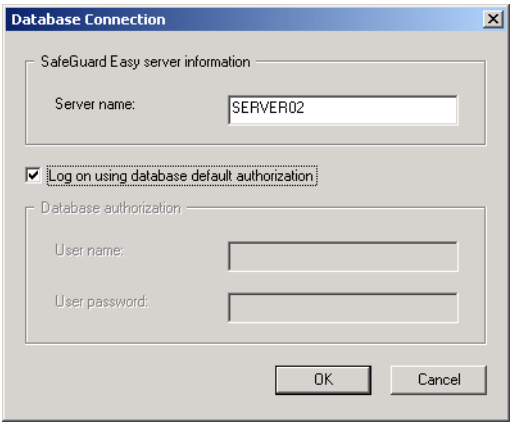
Prerequisites

- There must be a network connection between the new SafeGuard Easy Client and the SafeGuard Easy Server.
- SafeGuard Easy must be installed on the relevant SafeGuard Easy Client with the "Server Connection" option.
- The new SafeGuard Easy Client must not already be registered on the SafeGuard Easy Server. If the new SafeGuard Easy Client is already registered on the SafeGuard Easy Server, and really does need to be reregistered, you must first delete the Client entry from the database and then reregister it. To delete clients from the SafeGuard Easy Database, select the Workstations/Delete Workstations menu option.
- The Administration Console user must know the SafeGuard Easy access data for the new SafeGuard Easy Client.

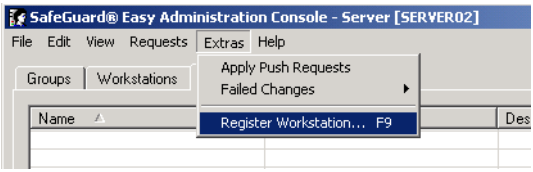
Procedure

1. Make sure there is a network connection between the Client and Server.

2. Start the Administration Console and log on to the database.

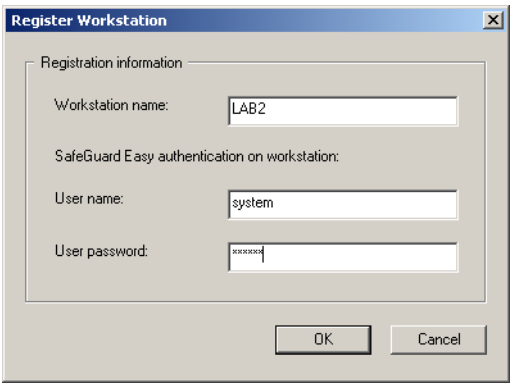


3. **Select the Extras/Register Workstation...** menu option.

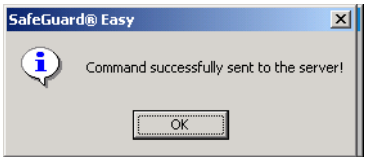


4. The system displays a dialog in which you are prompted to enter the name of the SafeGuard Easy Client and the authentication data for this Client.

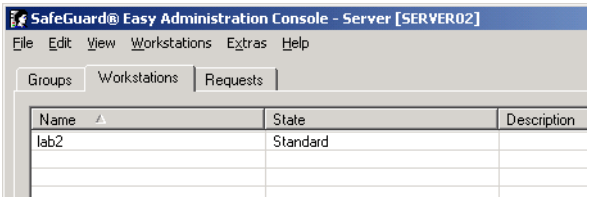
   The user profile of the SafeGuard Easy user whose name you have entered must exist on the SafeGuard Easy Client. The profile does not require any special SafeGuard Easy rights.



5. Click [OK] to confirm your entries. The system displays a dialog that confirms whether you have succeeded or not.



6. The Client then places information on the SafeGuard Easy Server. Depending on current network load, you might need to wait some time. After you have finished waiting, the new SafeGuard Easy Client is displayed in the Administration Console. (You can also update the display manually in the Administration Console by pressing [F5].



31.4.1 Re-registering several SafeGuard Easy Clients

The re-registering function works for every SGE Client from version 4.11 onwards.

Follow these steps to register several new SGE Clients:

1. Follow the Configuration File Wizard to create a new configuration file that has the "Install" property.
2. In this configuration file, enter the password specified for the SYSTEM user on the SGE client.
3. Save the configuration file as "SGEREG.cfg".
4. On the SGE client, copy the SGEREG.cfg file to the <system drive>/ System32 folder.
5. On the SGE Client, create two new Registry entries [DWORD values] in

   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   Sgeasy

   NotRegistered=1
   RegReport=1
6. Restart the SGE Client (or the SGE Service).

31.5 Registering SafeGuard Easy Clients on another SafeGuard Easy Server

If you want to administer SafeGuard Easy Clients on another SafeGuard Easy Server instead of the one on which they are currently registered, you can do so via the "registering on another server" function. For you to do so, a "registration request" is generated. The registration request is similar to a "normal" request, but instead of configuration updates it contains the new SafeGuard Easy Server name and SafeGuard Easy data for authentication on the SafeGuard Easy Clients that are to be "moved".

A registration request is processed more or less in the same way as a "normal" request: after the registration request is generated, the Administration Console adds it to in the queue. As soon as a SafeGuard Easy Client queries the "old" SafeGuard Easy Server, it finds the registration request there, and sends it to the "new" SafeGuard Easy Server. Following that the old SafeGuard Easy Server receives a report about the reregistration from SafeGuard Easy Client and the old SafeGuard Easy Server then removes the SafeGuard Easy Client from the "old" SafeGuard Easy Database.

NOTES:

The new SafeGuard Easy Server must not be registered as a SafeGuard Easy Client on the old SafeGuard Easy Server.

You can move individual SafeGuard Easy Clients, several at once, or groups of SafeGuard Easy Clients.

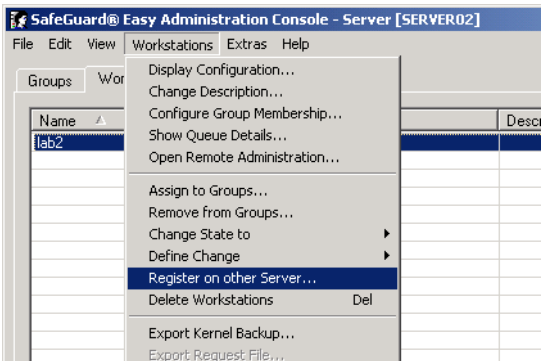
After the SafeGuard Easy Client has been successfully moved, the registration request is deleted since the SafeGuard Easy Client no longer exists on it. The registration request only remains in the queue until the point in time at which the registration request has the status "Waiting", "Planned" or "Failed".

Prerequisites

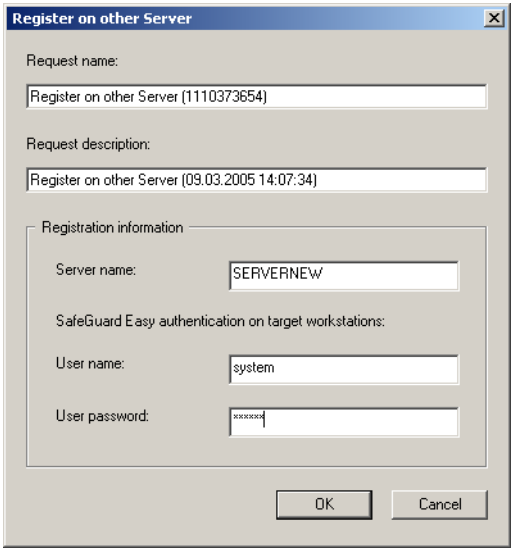
- There must be a network connection between the SafeGuard Easy Client and the SafeGuard Easy Server.
- The Administration Console user must know the SafeGuard Easy access data for the SafeGuard Easy Client.
- The SafeGuard Easy Client must already be registered on the old SafeGuard Easy Server (= must already be present in the SafeGuard Easy Database).

How to register SafeGuard Easy Clients on another SafeGuard Easy Server:

1. Start the Administration Console and log on to the database.
2. Mark the selected clients/groups.
3. **Select the Workstations/Register on other Server...** menu option.

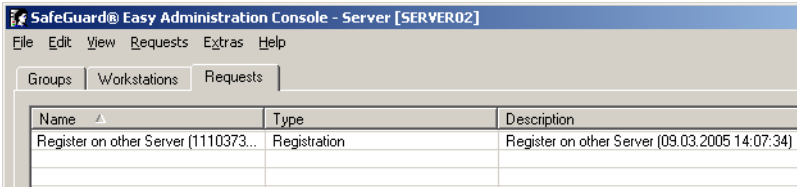


4. The system displays a dialog in which you are prompted to enter the name of the new SafeGuard Easy Server and the authentication data for the Client. We recommend you enter a meaningful Request name and Request description.
   The user profile of the SafeGuard Easy user whose name you have entered must exist on the SafeGuard Easy Client, but the profile does not require any special SafeGuard Easy rights.

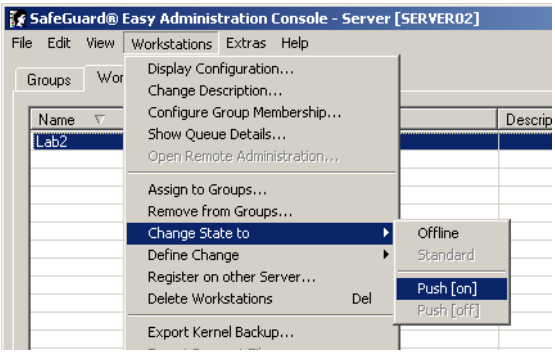


5. Click [OK] to confirm your entries.

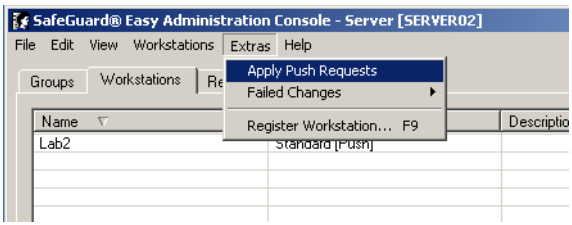
6. The registration request is displayed in the queue.



7. Select the **Workstations/Change State to/Push [on]** menu option to set the status of the SafeGuard Easy Client to "Push".

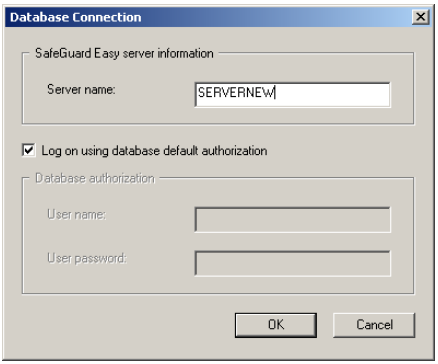


8. Select the **Extras/Apply Push Requests** menu option to start the registration request.

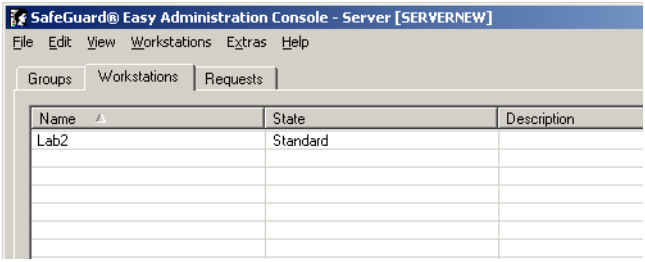


9. The system removes the SafeGuard Easy Client, its queue and other database dependencies from the old database.

10. Start the Administration Console and connect to the new SafeGuard Easy Server.



11. The system displays the reregistered SafeGuard Easy Client in the Administration Console.



31.6 Defining groups

The Administration Console administers the individual SafeGuard Easy clients that have registered themselves on the SafeGuard Easy Server. In large organizations, however, it is often sensible to gather the SafeGuard Easy clients in groups. This allows configuration settings to be distributed to a large number of PCs at once. Groups may be structured, for example, according to departments or may be formed because they have identical SafeGuard Easy settings. Even if clients are members of groups, you can set up specific configurations for them.

Within SafeGuard Easy groups there are no hierarchies. For example, you cannot specify that group A cannot contain group B, group C has no more rights than group D, etc. On the other hand, each SafeGuard Easy Client can be a member of many groups.

Grouping clients is very time-consuming in large organizations. During a pre-configured installation, a SafeGuard Easy parameter automatically assigns clients to one or more groups (see Parameter `Groups` in chapter 'SafeGuard Easy setup parameters').

SafeGuard Easy groups work independently of existing Windows user groups!

31.6.1 Creating/deleting groups

To create a group, click the **Groups** tab and select **Create Group**. You see a dialog in which you enter a group name. When you confirm your entry, it is displayed in the Groups tab list.

You can delete groups that are no longer required via the **Groups/Delete Group** menu option.

Even if a request has been deleted, it remains in the queue, and is carried out, if it has been sent for a group.

31.6.2 Assigning a SafeGuard Easy Client to a group/removing a SafeGuard Easy Client from a group

If you want to administer SafeGuard Easy clients by group, an existing group name must already be assigned to them. To do this, click the Workstation tab. In it, select a SafeGuard Easy Client and select the **Workstation** menu **Assign to Groups...** menu option. Select a group and confirm your selection.

To remove a Client from a group, select the **Workstation/Remove from Groups...** menu option.

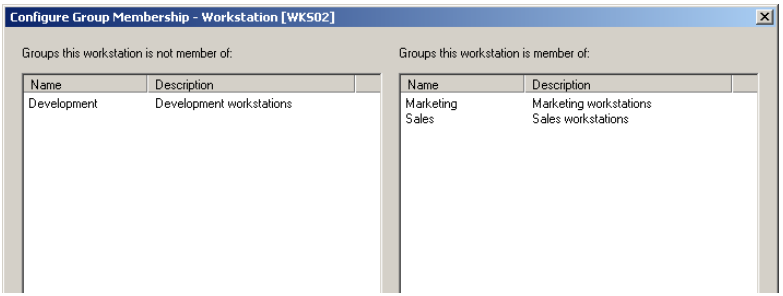
You should not change group memberships until all existing requests have been carried out!

31.6.3 Finding out group membership

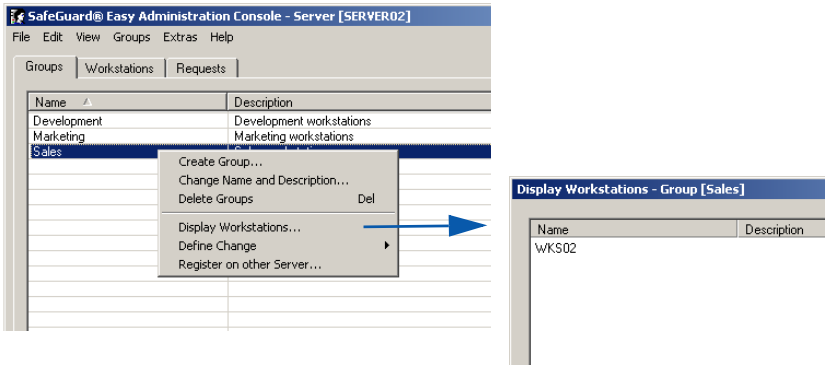
Administrators need a quick way to check group memberships so that they can ensure that clients are always supplied with correct data.

The Administration Console provides this data in the following ways:

- **Workstation/Configure Group Membership...**
  Use this menu option to check the group membership of a SafeGuard Easy client. You can use the direction keys to change the group membership.



- **Groups/Display Workstations:**
  Use this menu option to list the members of a group.



31.6.4 Changing a group name

To change a group name, select the **Change groups** menu option in the **Groups** menu. Enter the new group name and confirm it by clicking OK.

31.6.5 Removing groups

To remove a group, select the **Delete Group** menu option in the **Groups** menu.

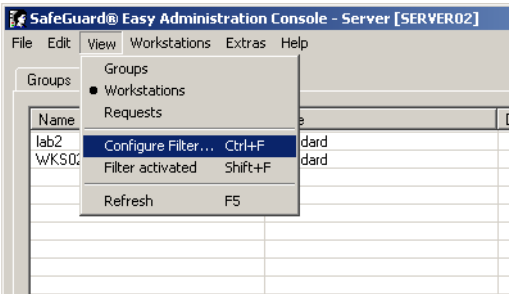
31.7 Defining rules for displaying workstations/groups/requests

The Administration Console has a filter function with which the Administrator can specify exactly which SafeGuard Easy clients, groups or requests they see on the screen. This procedure is useful if there are a large number of objects to manage, as it makes administration easier and also makes it easier to see what is going on.

You access the filter definition dialog in the **View** menu in each tab.

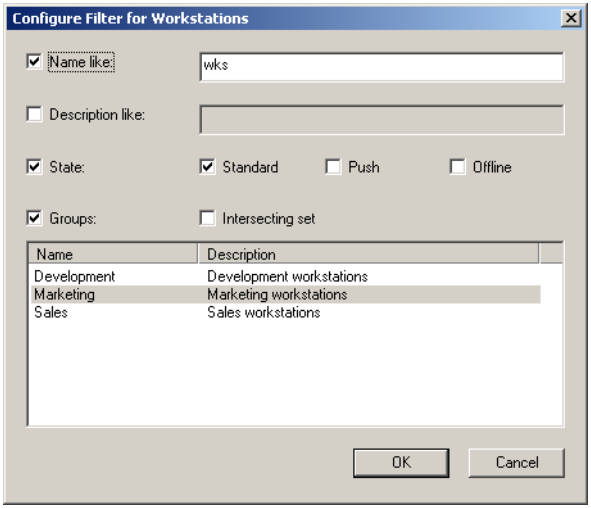
You define the filter in two steps:

- Configure a filter
- Activate the filter



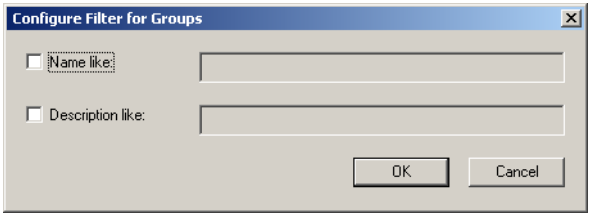
31.7.1 Configuring a filter

You can define a wide range of rules to make *workstations* visible/invisible. With an extended option you can even define the intersection of selected groups as a rule (i.e. workstations will only be displayed if they are a member of group A and group B).

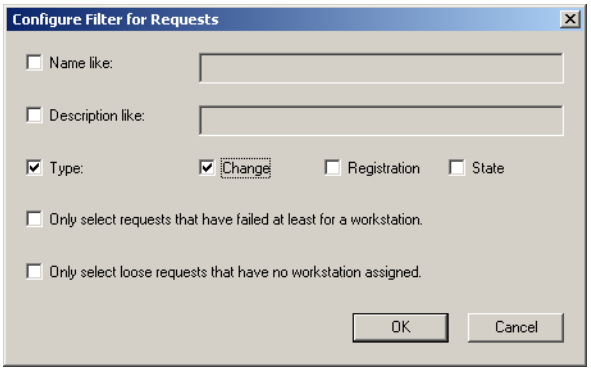


View for workstations

For *groups and requests* you can filter by name and description. For requests you can also display only failed requests.



View for groups



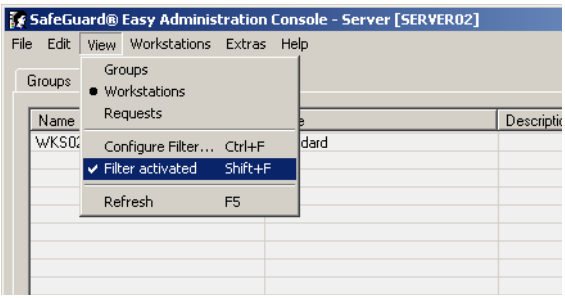
View for requests

In the "Name like" and "Description like" fields you can also use a wildcard, but the only accepted wildcard character is "*" (asterisk). This means that, at the position containing the character "*", several different characters may be present in the Name or Description columns.

Generally the following rule applies: only workstations/groups/requests that match all of the selected properties are displayed.

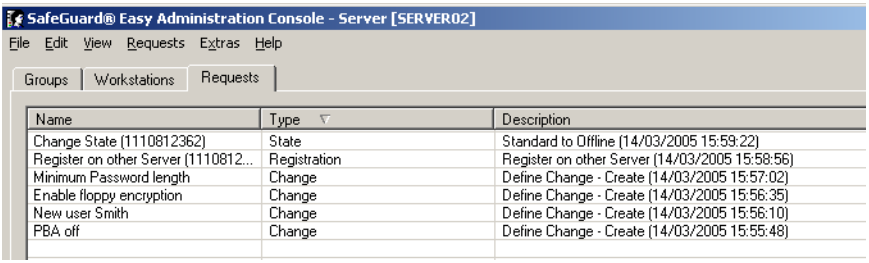
31.7.2 Activating a filter

The filter only takes effect when it has been activated. You can tell you are working in Filter mode by the changed color of the user interface in the Administration Console. For example, the default white background changes to blue.



31.8 Requests and Queues

Requests contain configuration updates for SafeGuard Easy clients. The SafeGuard Easy Client fetches these updates from the SafeGuard Easy Server as soon the two devices are communicating with each other. If a SafeGuard Easy Client finds current changes, it lists them in accordance with the sequence in which they were assigned to the Client via the Administration Console. Once requests have been created they can be applied as often as required for different groups/workstations. All sent requests are grouped in the queue in the "Requests" tab, no matter what their status is.


SafeGuard® Easy Administration Console - Server [SERVER02]
File Edit View Requests Extras Help
Groups Workstations Requests
Name Type Description
Change State (1110812362) State Standard to Offline (14/03/2005 15:59:22)
Register on other Server (1110812... Registration Register on other Server (14/03/2005 15:58:56)
Minimum Password length Change Define Change - Create (14/03/2005 15:57:02)
Enable floppy encryption Change Define Change - Create (14/03/2005 15:56:35)
New user Smith Change Define Change - Create (14/03/2005 15:56:10)
PBA off Change Define Change - Create (14/03/2005 15:55:48)

A request corresponds broadly to the function of a configuration file (see 'Creating a new configuration file') and makes changes to the existing SafeGuard Easy settings for a particular client. A change might involve a small alteration in the configuration of the SafeGuard Easy Client or even the uninstallation of SafeGuard Easy. On the other hand, it is not possible to use requests to carry out installations. If required, requests also integrate existing configuration files.

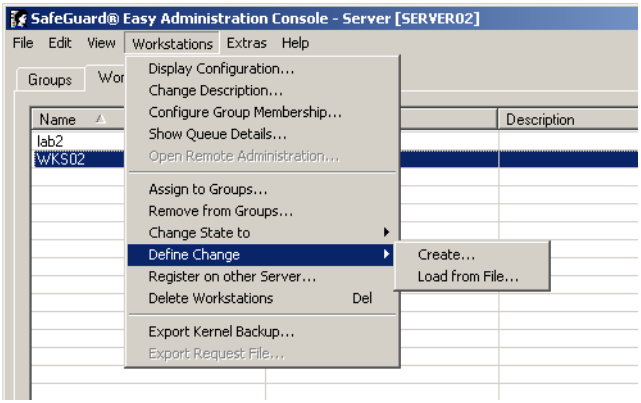
The success/failure of a request is immediately transmitted to the Server so that the administrator is always kept fully informed of the current status. A request is only carried out successfully if the creator data (SafeGuard Easy User name and Password) match the user data of a SafeGuard Easy user on the SafeGuard Easy Client. In addition the rights profiles of the creator must allow the specified changes to be made on the Client.

Requests are placed in a server **queue** according to their creation date, and wait there until they are fetched by the Client. Clients always fetch the request with the oldest creation date first.

31.8.1 Creating changes (requests)

New requests can be created for individual SafeGuard Easy clients or for groups. If a SafeGuard Easy Client is a member of several groups, the request is still only carried out once for that client.

You can generate a new request via the **Define Change** menu option, which you will find both in the **Workstation** menu and the **Groups** menu.

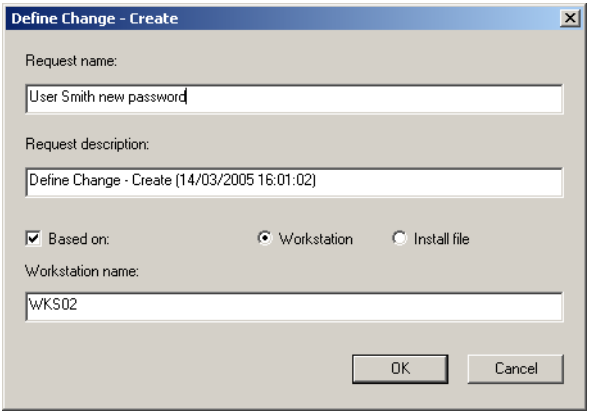


When you select **Define Change**, you can choose between:

- **Create...**
  Generates a new request
- **Load from File...**
  Uses an existing configuration file as a request.

31.8.2 Creating a new request

If you select the **Workstation (Groups)/Define changes/Create** menu option, you see a dialog in which you preselect whether a request is created using a template (a so-called "base configuration") or not.



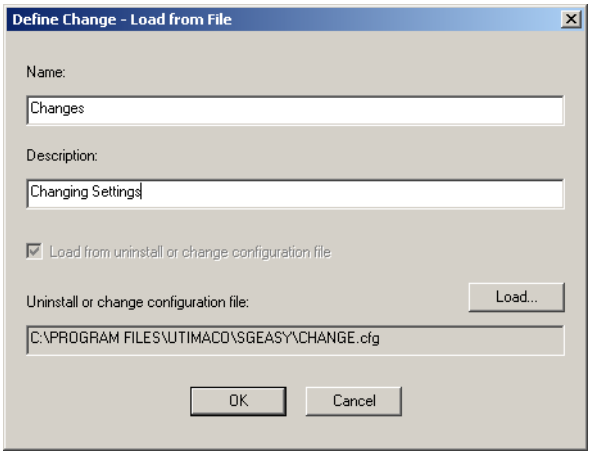
It is useful to use a template if it contains settings that are only slightly different from the planned request. It makes your work as an administrator easier by reducing the amount of options you need to type in or click. The request is based either on the settings of a client registered on the SafeGuard Easy Server (in which case you type in something like "WKS-") or you loaded the data for the request from a configuration file with the attribute "Install". With this function you can, for example, copy settings from one machine to another.

If you do not use a template, a new request is created that does not take its settings either from a configuration file or from a workstation.

When you confirm your dialog entries the Configuration File Wizard starts (see 'Configuration File Wizard'). If the Configuration File Wizard recognizes an Install configuration file as a basis for a request, it requires authentication before all data can be displayed.

31.8.3 Using an existing configuration file as a request

You can also select the **Workstation (Groups)/Define changes/Load from file** menu option to assign an existing configuration file directly to a request. This configuration file might for example uninstall SafeGuard Easy from a SafeGuard Easy Client, or simply make changes. The prerequisite for this to work is that this file has already been created with the Configuration File Wizard.



The "life expectancy" of existing configuration files determines whether you work with them. Requests without an assigned configuration file are not available as individual files, when they are complete. Instead they are stored as links in the SafeGuard Easy Database. Once they have been successfully carried out, you cannot edit their settings or assign them to other workstations!

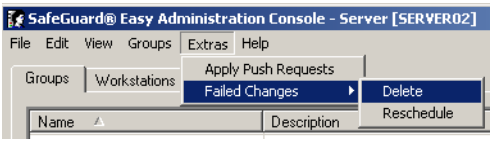
31.8.4 Failed requests

Requests can fail

- if the rights profiles of the request creator do not permit the change entered in the request to be carried out on the SafeGuard Easy Client. If at least one setting change in the change request cannot be made, the whole changes request will not be carried out!
- if the request creator fails to authenticate themselves on the SafeGuard Easy Client.
- if for some reason there is no network link between the SafeGuard Easy Client and SafeGuard Easy Server (in urgent cases we recommend that you use the Offline clients procedure instead).
- if entries in the request do not match with the SafeGuard Easy settings on the Client (for example, incorrect SafeGuard Easy password entered for a SafeGuard Easy user in request).

A failed job stops the processing of other jobs in the queue. Also, for example, it is not possible to save request files for offline clients if a job fails.

As soon as the failed job is removed from the queue or added again to the queue all other jobs will be executed. To remove failed jobs or add them again, select the **Extras/Failed changes menu option.**



31.8.5 Changing a request name

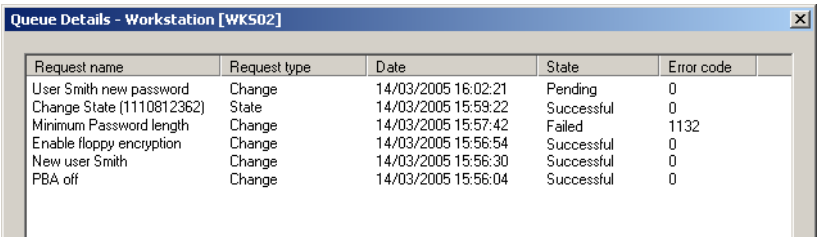
You can give a new name and description to a request displayed in the "Requests" tab by selecting **Requests/Change name and description**. The changed entries are applied immediately.

31.8.6 Deleting a request

As long as a request has not yet been carried out, you can undo unwanted changes again. To do so you must remove the request from the queue. If you select a request, and then select the **Requests/Delete request** menu option, the request will be deleted and removed from the queue.

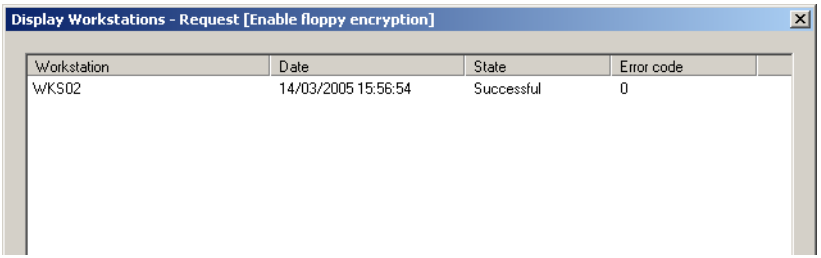
31.8.7 Displaying a queue

In the general queue (**Workstation/Show Queue details**) menu option you will find a list of all requests for particular SafeGuard Easy clients, their current status (successfully carried out, failed, etc.) and details of when the request was created.



NOTE:
The [Delete] button can only be used if none of the selected entries is in "Pending" mode.

In the request-specific queue (**Requests/Display Workstations** menu option) you will find a list of requests successfully processed per workstation, or still in the queue.



The jobs in a queue can have the following properties:

- **Successful:** The request was carried out on the SafeGuard Easy Client and the Server has received a message to confirm successful completion.
- **Failed:** The request was carried out but there was an error in doing so, and the Server was been informed. The meaning of the displayed "Error number" is described in the "Error Messages" chapter.
- **Pending:** The request has been sent to the SafeGuard Easy Client but the Server has not yet received a message to say whether it was successfully carried out, or failed.
- **Scheduled:** The request is waiting to be sent to the SafeGuard Easy Client. This status occurs as soon as the SafeGuard Easy Client contacts the Server or if the queue is put in Push mode.

31.9 State of a SafeGuard Easy Client

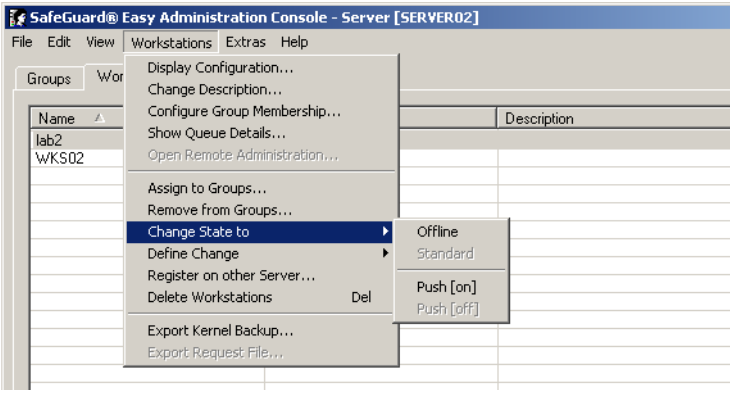
The state of a workstation describes the type of link between the SafeGuard Easy Server and SafeGuard Easy Client. The state also specifies how the SafeGuard Easy Server processes the workstation queue.

Workstations can have different states:

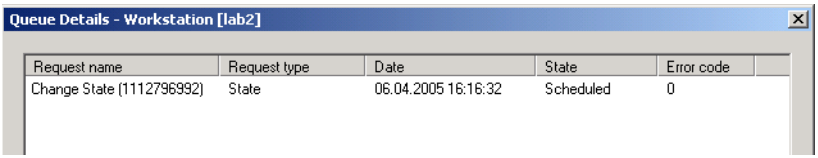
- Standard (online)
- Offline
- Push on
- Push off

The states (Standard/Online and Offline) show the type of connection between the SafeGuard Easy Server and SafeGuard Easy Client, and consequently also define the way that the SafeGuard Easy Server and SafeGuard Easy Client communicate. "Push on" and "Push off" can be combined with the other two states (Standard/Online and Offline). Workstations with the attribute "Push (on)" are the workstations whose queues are to be processed by the SafeGuard Easy Server immediately after a command runs in the Administration Console.

You can select the **Workstations/Change State to** menu option to change the status.



As soon as a SafeGuard Easy Client's state is changed (to Standard or Offline), SafeGuard Easy adds a "State Request" to the queue.



31.9.1 State "Standard (Online)"

Every Client has the state "Standard" after it has exchanged communications information with the SafeGuard Easy Server (key pair, GUID generation, assignment of the SafeGuard Easy server name) and has then registered on the Server for the first time. Clients with the attribute "Standard" are PCs that regularly make contact with the network (for example, stationary PCs in office buildings). These SafeGuard Easy clients always autonomously make contact with the Server and fetch the requests intended for them each time they make contact with it, first when the SafeGuard Easy Client boots, and then every 6 hours.

31.9.2 State "Offline"

Offline clients are PCs that, as is known in advance, never connect with the network or the SafeGuard Easy Server (such as notebooks used by sales representatives), but nevertheless need to be administered centrally. You install SafeGuard Easy on these PCs in the normal way, with initial registration on the SafeGuard Easy Server. In the Administration Console the administrator then switches the state of the relevant client to "Offline". The administrator only does so if they knows the client will not autonomously attempt to contact the network. Failed queries from the Client to the Server, or similar, do *not* indicate that the Client is "Offline".

You can assign "Offline" state to a Client during installation by entering the server name ".OFFLINE".

"Offline" state also has effects on the handling of requests created for the PC set to Offline, which are to be carried out on it. If the administrator creates one (or more) requests for the Client, they are placed in the queue but are never fetched by the SafeGuard Easy Client, since there is no link to the SafeGuard Easy Server.

Despite this missing client/server link, an Administration Console function transfers all the for one Offline Client in one file. The administrator sends this file by e-mail to the user of the Offline client, who imports the file using a tool supplied with SafeGuard Easy. Once requests have been saved in a request file they are assigned the status "Pending" in the server queue. This prevents them from being added to request files later. As soon as the request file has been imported, the requests are processed in the specified sequence on the offline PC.

As the administrator has no contact with the Offline Client, they do not know whether the changes have been made successfully, or failed. This missing information is provided in a report file which is generated after the request file has been processed. This file is passed to the administrator, and needs to be imported into the Administration Console (where a suitable import function is provided for that purpose). After the import the administrator can see whether the configuration changes have been successful or not by viewing the properties of the Offline client.

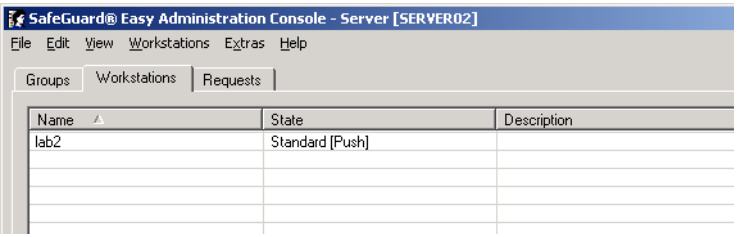
A Client can only change from Offline to Standard state if it has been installed using the Server Connection option and knows the SafeGuard Easy Server name.

It is not only Offline clients that can exchange request or report files. If, for example, the network link between SafeGuard Easy clients and the SafeGuard Easy Server fails, this procedure can be used to pass on configuration changes to the unreachable clients until the clients can be centrally administered again.

31.9.3 State "Push [on]"

A SafeGuard Easy Client can be forced to synchronize its settings first with the Server and then will all other clients. This can be relevant if a user wants a particular configuration or the administrator needs to load immediate changes on the Client (if, for example, a member of staff leaves the company and their access to the Client needs to be blocked).

The SafeGuard Easy Client is assigned the attribute "Push", e.g. "Standard [Push]" so that the SafeGuard Easy Server knows which SafeGuard Easy Client is meant. To do this, select the **Workstations/ Change State to/Push [on]** menu option.

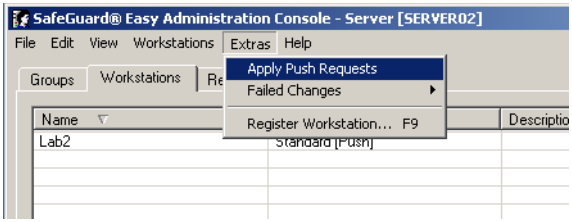


When you have selected the Extras/Apply Push Requests menu option, a client's "Push" attribute wakens the Server, which is usually in a passive state, waiting for queries from the clients. The SafeGuard Easy Server makes one autonomous attempt to contact the Client with the attribute "Push" and process all jobs, with the state "Planned", that are present in the queue for this Client, until the queue is empty or a job fails. In both cases the Server then returns to the passive (normal) state back and remains in it until the Administrator "pushes" it again.

The "Push" attribute is also automatically removed at the same time.

The push mechanism is a compromise between network load and security.

If you do not want Push mode to apply immediately, you can initiate contact between the SafeGuard Easy Server and Clients later by selecting the **Extras/Apply Push Requests menu option**.



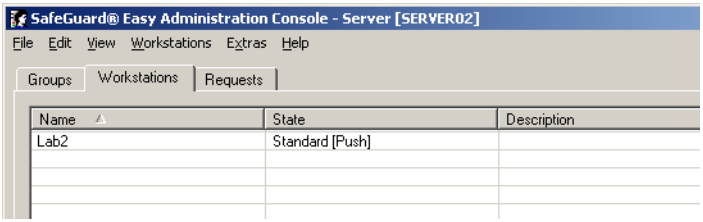
31.9.4 State "Push [off]"

Select the **Workstations/Change State to/Push [off]** menu option to switch off the SafeGuard Easy Client's Push attribute.

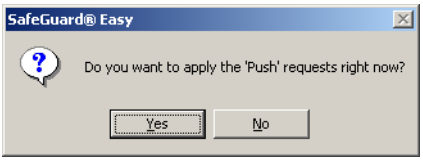
31.9.5 Switching the SafeGuard Easy Client from Standard (Online) to Offline mode

1. Select the **Workstations/Change State to** menu option.

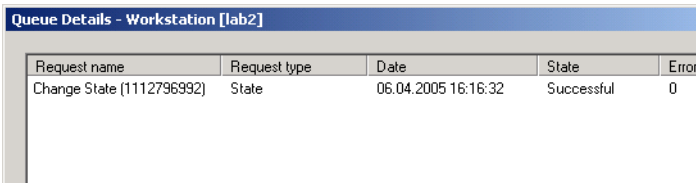
   Set State to
   a) Offline
   b) Push [on]


SafeGuard® Easy Administration Console - Server [SERVER02]
File Edit View Workstations Extras Help
Groups Workstations Requests
Name State Description
Lab2 Standard [Push]

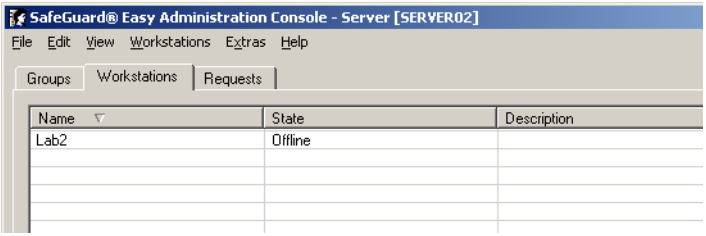
2. If you want the SafeGuard Easy Client to enter OFFLINE mode immediately, click [Yes] in the dialog you see next.



3. In the SafeGuard Easy Client's queue a request is created with the state "Successful".

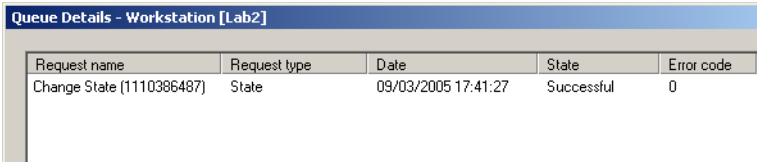

Queue Details - Workstation [lab2]
Request name Request type Date State Error
Change State (1112796992) State 06.04.2005 16:16:32 Successful 0

4. The SafeGuard Easy Client now has the state "Offline".

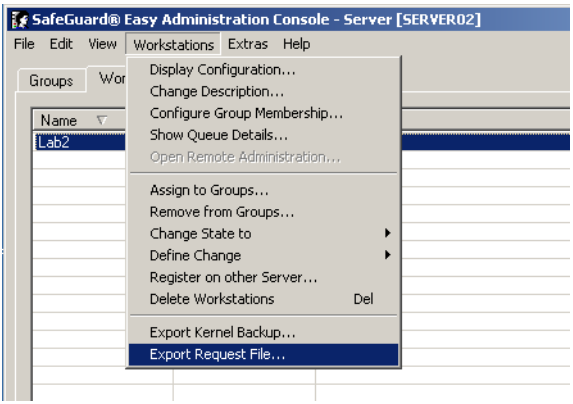

SafeGuard® Easy Administration Console - Server [SERVER02]
File Edit View Workstations Extras Help
Groups Workstations Requests
Name State Description
Lab2 Offline

31.9.6 Generating configuration updates for offline clients in the Administration Console

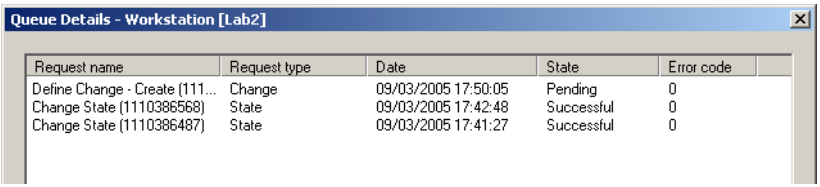
1. The SafeGuard Easy Administrator uses the **Workstations/Define Change** menu option to create a configuration update ("change request"). In the queue each request is set to "Planned".



2. The SafeGuard Easy administrator selects the **Workstation/Export Request File...** menu option to export the request in a "request file" (file extension .req).

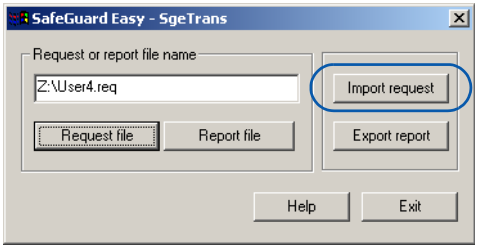


3. Once a request file has been created, the status of the request in the queue changes to "Pending".



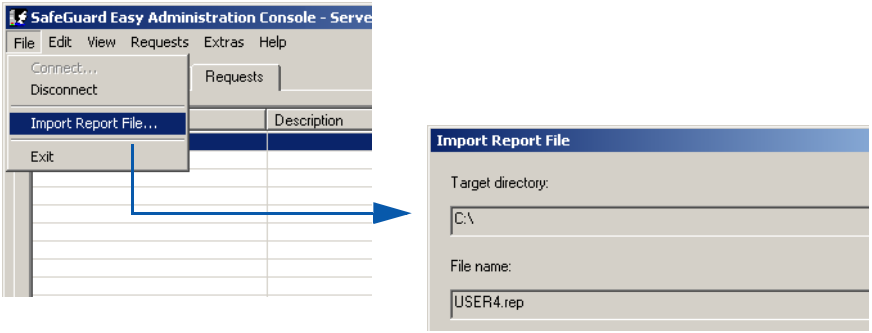
4. The SafeGuard Easy Administrator sends the request file to the user of the Offline client, for example via e-mail.

5. The user of the Offline client imports the request file with SafeGuard EasyTrans (see 'Loading a configuration update onto an Offline Client with SGETRANS').

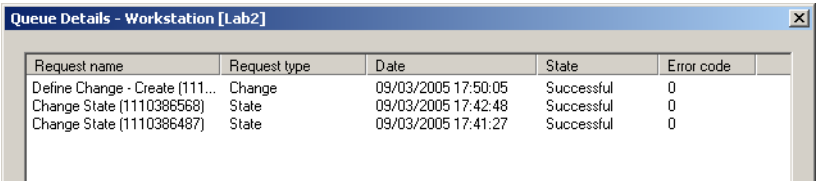


6. SafeGuard Easy tells the user of the offline client whether the change file has been successfully executed or not.
   At the same time, a "report file" (file extension .rep) is generated on the Offline Client, and the user sends it to the SafeGuard Easy Administrator.

7. The SafeGuard Easy administrator selects the **File/Import Report File...** menu option to import the report file into the Administration Console.

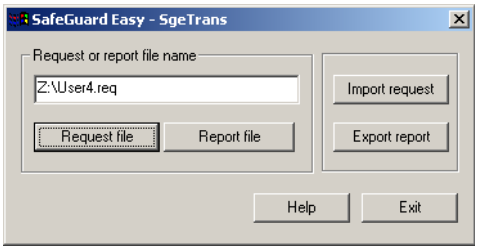


8. The SafeGuard Easy Administrator can view the queue (or the Properties page for the workstation) to see whether the changes have been successfully carried out.


Queue Details - Workstation [Lab2]
Request name | Request type | Date | State | Error code
Define Change - Create (111... | Change | 09/03/2005 17:50:05 | Successful | 0
Change State (1110386568) | State | 09/03/2005 17:42:48 | Successful | 0
Change State (1110386487) | State | 09/03/2005 17:41:27 | Successful | 0

31.9.7 Loading a configuration update onto an Offline Client with SGETRANS

The SGETrans.exe application acts as an interface for exchanging Request and Report files while working with Offline clients. SGETrans is only available in the SafeGuard Easy folder if the "Server connection" option was chosen during the Client installation.



- **Request file**
  Loads the request file, which the user got from the administrator (for example by mail).
- **Import request**
  Saves the settings of the request file on the user workstation.
- **Report file**
  Defines a file name for the report file.
- **Export report**
  Saves the Report file, which the user sends to the administrator.

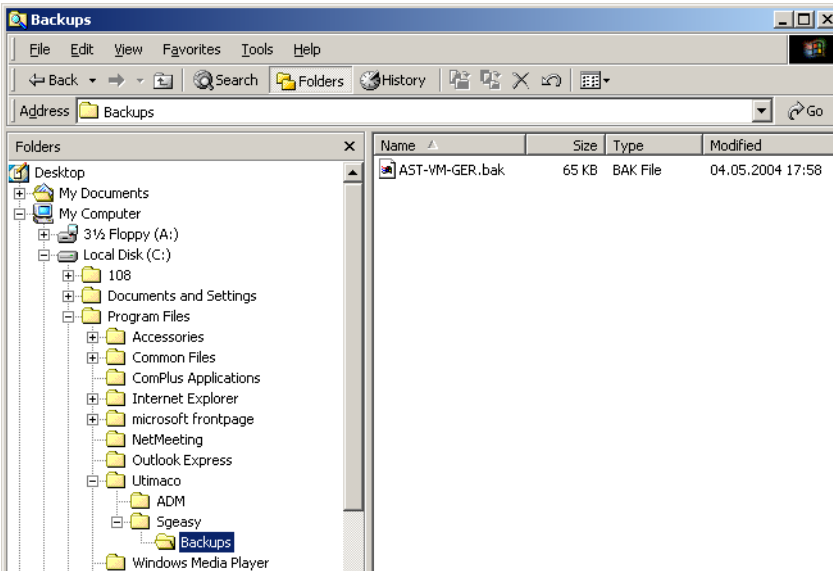
31.10 Automatic system kernel backup

The system kernel contains all the necessary functions for authentication on the computer, the drivers necessary for starting an operating system, and all system settings for a SafeGuard Easy client. An up-to-date backup is needed in emergency situations in particular, if the system kernel of a SafeGuard Easy client has been damaged and the user can no longer log on to the system. In such cases an intact system kernel is needed for the workstation involved, so that the original state can be restored and the system can be enabled to run again ('Creating emergency media and saving the system kernel').

Automatic system kernel backup means the administrator no longer has the task of reminding users to make the necessary backups, or even have to carry them out personally. Instead this task is taken on by an auto-backup function as part of central administration. After the SafeGuard Easy Client successfully registers with the SafeGuard Easy Server, the auto-backup function causes it to send a system kernel backup to the SafeGuard Easy Server. Even if changes are made to the SafeGuard Easy configuration (for example via executed configuration files), the SafeGuard Easy Client generates the backup, sends it to the server and overwrites the old data. The auto-backup guarantees that the administrator can act independently of user backups, which may or may not be present, in emergency situations.

31.10.1 Backing up the system kernel into the Backups folder

By default SafeGuard Easy places the saved system kernel in the SafeGuard Easy folder on the machine on which the SafeGuard Easy Database is located (usually the SafeGuard Easy Server).
There, a \Backups folder is specially generated, and the system kernels are copied into it. It is very easy to see how the backups are assigned to the workstations: the file name consists of the name of the registered workstation and the extension .bak.



31.10.2 Creating a new backup folder

In the Registry enter **BackupDirectory** in

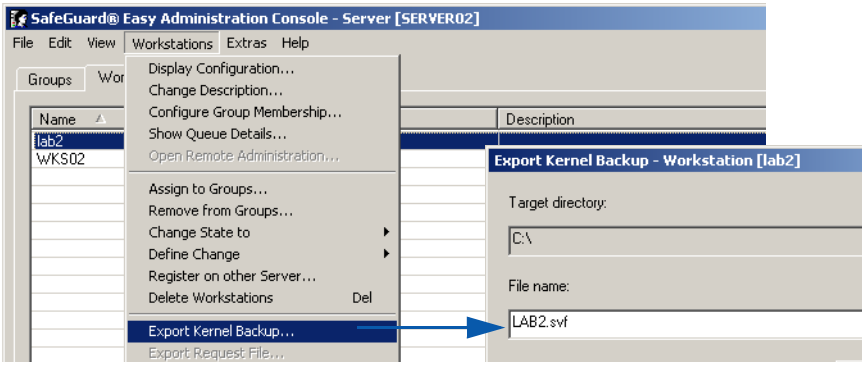
HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
Sgeasy

you can specify a new folder for the backups. You will then need to reboot the PC. In general it is possible to enter a local or a UNC path. If you enter a UNC path, ensure that there are sufficient rights ("Change").

You must set this registry key on the PC on which the SafeGuard Easy database is located.

31.10.3 Exporting the system kernel

You can also export the system kernel backups for all SafeGuard Easy clients directly, via the Administration Console. To save a backed-up system kernel, select the **Workstations**/**Export Kernel Backup**... menu option. Here you can select the target folder, file name and file extension to suit your needs.



Pass the file to the user on whose PC a system error has occurred. To find out how to use an intact system kernel to fix system errors on a workstation, see Chapter 'Creating emergency media and saving the system kernel'.

32 Remote Administration

In Remote Administration the administrator links to one specific SafeGuard Easy Client from the admin workstation and modifies the SafeGuard Easy configuration on the client as required. The administrator feels as if they were sitting right in front of the SafeGuard Easy Client and making the changes locally.

Some changes via Remote Administration, such as enabling encryption/decryption, have an immediate effect on the SafeGuard Easy Client, while others require the SafeGuard Easy client to be re-booted.

Remote Administration works independently of central administration and is ideal for admin tasks in smaller networks. It can be used on a stand-alone basis or as an integral element of the Administration Console. The administrator can use it to carry out the following tasks:

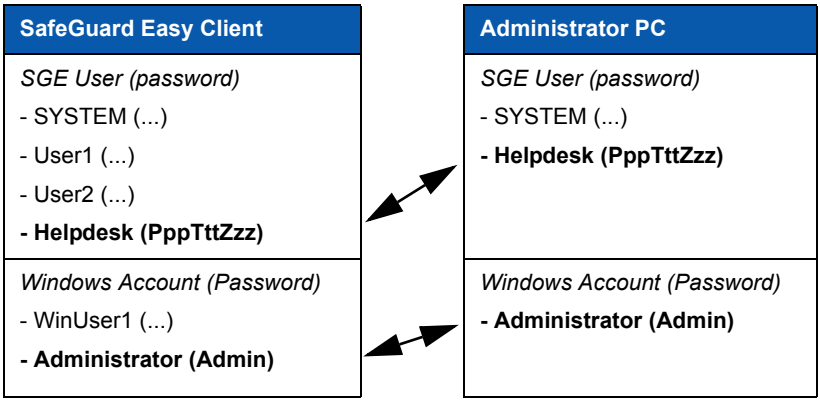
- Linking to a SafeGuard Easy Client
- Authentication on the SafeGuard Easy Client
- Changing the settings for the SafeGuard Easy client
- Displaying encryption/decryption processes on the SafeGuard Easy Client
- Saving settings
- Initiating backup of the SafeGuard Easy client's system kernel.

Remote Administration is integrated in the familiar SafeGuard Easy Administration functionality and uses its existing administration tools.

32.1 Prerequisites

You can only use the Administrator PC to view and change settings on a SafeGuard Easy Client if the following apply:

- there is a network link between the Administrator PC and the SafeGuard Easy Client.
- the Windows account (user ID and password) with which the administrator has logged on to the Administrator PC exists on the Administrator PC and the SafeGuard Easy Client. When the link is set up, the administrator is automatically logged on to the SafeGuard Easy Client.
- at least one identical SafeGuard Easy user (including password) is held on the SafeGuard Easy Client and the Administrator PC.
- the user of the Administrator PC uses exactly the same SafeGuard Easy user information to log on to SafeGuard Easy Administration with integrated Remote Administration.

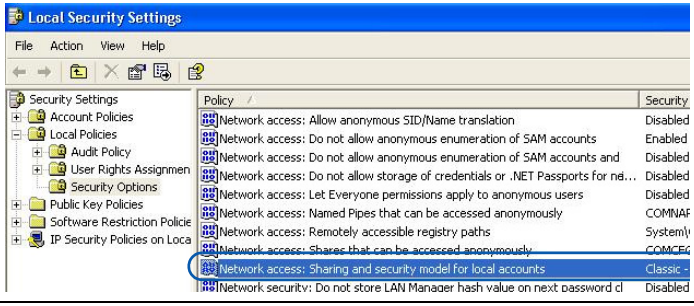


The SafeGuard Easy user on the Administrator PC can only perform the tasks for which they have authorization, according to their user profile!

NOTE:

The Windows XP operating system requires the following Local Security Setting on client and/or Administrator workstation:

"Network access: Sharing and security model for local accounts = Classic - local users authenticate as themselves".The Local Security Settings are opened via Control Panel/Administrative Tools/Local Security Policy.


Local Security Settings
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignmen
Security Options
Public Key Policies
Software Restriction Policie
IP Security Policies on Loca
Policy
Security
Network access: Allow anonymous SID/Name translation
Disabled
Network access: Do not allow anonymous enumeration of SAM accounts
Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and
Disabled
Network access: Do not allow storage of credentials or .NET Passports for ne...
Disabled
Network access: Let Everyone permissions apply to anonymous users
Disabled
Network access: Named Pipes that can be accessed anonymously
Network access: Remotely accessible registry paths
Network access: Shares that can be accessed anonymously
Network access: Sharing and security model for local accounts
Classic -
Network security: Do not store LAN Manager hash value on next password cl
Disabled

32.2 Installing Remote Administration

To perform remote configuration on the SafeGuard Easy clients it is necessary to install Remote Administration on the computer (Administrator PC) from which you would like to configure the SafeGuard Easy clients.

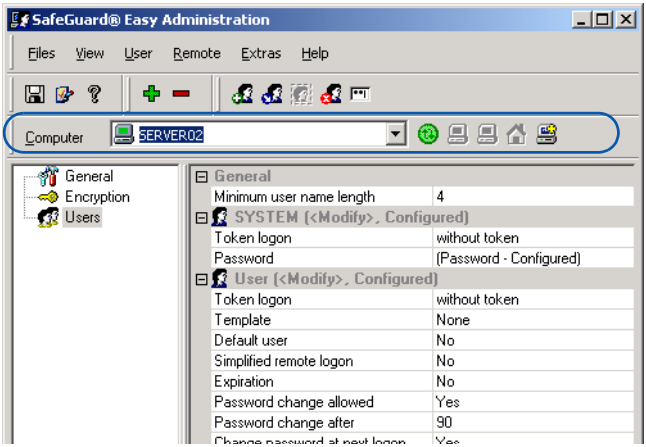
Installation involves these steps:

1. Run `Sgeasy.msi` in the \CLIENT folder on the CD. Select installation type "Standard".

2. Run `Server.msi` in the \SERVER folder on the CD. Select the "Remote Administration" option.

3. Ensure that there is a network link between the Administrator PC and user PC.

4. Select the Start / Programs / Utimaco / SafeGuard Easy / Administration menu option to start Remote Administration.



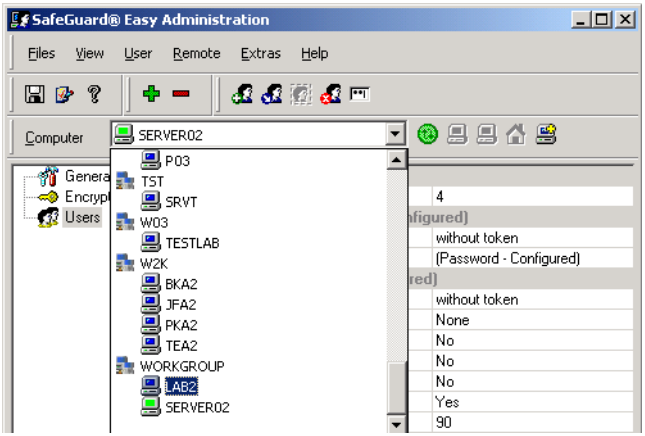
After you have installed Remote Administration, the following functions will have been added to SafeGuard Easy Administration:

- Select clients via a computer list
- Update computer list
- Create/close link with the client
- Enter a client name, which is not in the computer list, manually.

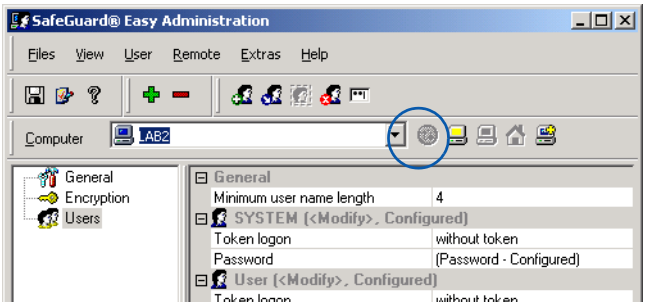
32.3 Establishing a connection to a SafeGuard Easy Client

1. User of the Administrator PC logs on to SafeGuard Easy's Administration.

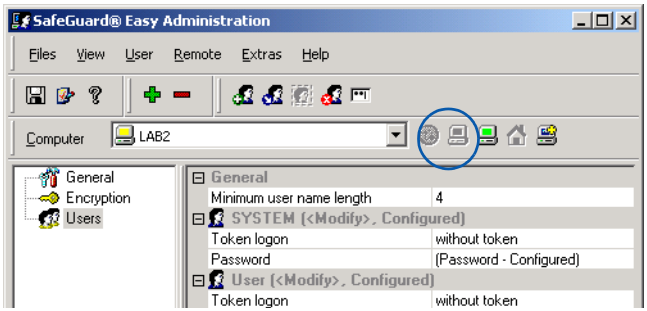
2. When the computer list is opened you can see the PCs (and also the domains) connected to the network.



3. The PC in green is the Administrator PC. If you select a client in the list, and then click the icon with a yellow PC on it, you create a link between the Administrator PC and SafeGuard Easy Client.



4. Once the link has been established, you automatically log on to the SafeGuard Easy Client with the ID of the SafeGuard Easy user who was locally authenticated when SafeGuard Easy's Administration was started (in our example its the Helpdesk profile).



5. If the attempt to log on using this SafeGuard Easy user ID has not been successful, the user is prompted to enter valid user data.

33 Error messages

The list of error messages is sorted according to error numbers. As each SafeGuard Easy error message is displayed with an error number, you can find the description required easily.

All the error messages have the following format: SGEnnnn: <text>

'SGE' is the SafeGuard Easy product ID, and 'nnnn' is a four-digit error number.

You will find more information on this subject in the Utimaco Knowledge Database http://www.utimaco.com/myutimaco.
In the "Knowledge database" section you will find more detailed information about the following SafeGuard Easy errors:
0104, 0113, 0400, 0401, 0404, 1048, 1062, 1074, 1089, 1104, 1109, 1121, 1123, 1244, 1254, 1264, 1274, 1306, 1315, 1509, 1602.
Use the Knowledge database's "Search" field to look for key words like "Error message" or type in a error number.

Real mode errors

0001	Fatal Error.
0002	Retry.
0100	Different version of [PN] or Crypton already installed.
0101	Cannot read configuration file.
0102	Invalid configuration file.
0103	Cannot write configuration file.
0104	Currently installed driver is inconsistent.
0105	Driver already installed.
0106	This program cannot be run under &0.

0107	Cannot write backup file.
0108	Cannot read backup file.
0109	Invalid backup file.
0110	Cannot install a second boot partition on disk.
0111	Cannot install on top of OS/2 Boot Manager.
0112	Earlier version of [PN] or C:CRYPT already installed.
0113	Last install, uninstall, or update not complete.
0114	Not enough contiguous free disk space on boot partition.
0115	Cannot access the driver boot partition.
0116	No resource files found.
0117	Cannot open resource file.
0118	Bad or unreadable resource file.
0119	Missing algorithm module.
0120	Missing kernel module.
0121	Missing PBA module.
0122	Cannot create *AUTOUSER.
0200	Cannot analyze hard disk structure.
0201	Hard disk read failure.
0202	Hard disk write failure.
0203	Invalid partition table on disk 0.
0204	Incompatible ROM BIOS.
0205	Invalid boot sector.
0206	Cannot lock volume.
0300	Disk write protected.
0301	Unknown unit.
0302	Drive &0 not ready.
0303	Unknown command.
0304	Data CRC error.
0305	Bad request structure length.

0306	Seek error.
0307	Unknown media type.
0308	Sector not found.
0309	Printer out of paper.
0310	Write fault.
0311	Read fault.
0312	General failure.
0320	Out of memory.
0321	Divide trap at program address &0.
0322	Runtime stack overflow.
0500	Encryption driver not installed.
0501	Incorrect encryption driver version.
0502	Invalid command line argument(s).
0503	No encryption key defined.
0999	Unknown error.

System API errors

1001	No subsystem active.
1002	Invalid change of a system setting.
1003	Invalid or missing encryption algorithm.
1004	Internal error in subsystem detected.
1005	Subsystem has reported an I/O error.
1006	The access to the kernel has failed.
1007	A user has already logged in to [[FILELINK]=SGE_INFO.DLL][[MSGLINK]=102].
1008	An invalid user was defined.
1009	Assigning defined rights to user is not allowed.
1010	Defined user already exists.

1011	The new password was already used for this user in the past.
1012	The new password belongs to list of not allowed passwords.

Common File errors

1031	File %1 cannot be opened.
1032	File %1 cannot be closed.
1033	File %1 cannot be created.
1034	Error writing to file %1.
1035	Error reading from file %1.
1036	Access to file %1 has failed.
1037	File %1 could not be found.
1038	Invalid path or filename defined.
1039	Not enough free space on disk.
1040	Hard disk partition is too heavily fragmented.
1041	Invalid file system detected.
1042	Unknown file system detected.
1043	File %1 already exists.
1044	Corrupted structure of the file system detected.
1045	Invalid entry in file system found.
1046	Request for partition information failed.
1047	Unknown or invalid file system detected.
1048	File %1 could not be copied.
1049	File %1 could not be deleted.
1052	CRC check for file %1 has failed.
1053	File %1 could not be renamed.

Installation errors

1061	Invalid installation drive.
1063	SafeGuard Easy system is already installed.
1064	Twinboot installation is not allowed for a system with more than one hard disk.
1065	The Config.sys file is write protected.
1066	Entry in INI file or configuration file not found.
1067	A complete or a runtime system of [PN] cannot be installed on a system with dynamic disk drives.\n\n Only administration utilities can be selected for installation.
1068	The kernel file could not be created.
1069	Config.sys file could not be modified.
1070	File %1 could not be copied.
1071	No target directory was defined.
1072	A wrong system administrator password was specified.\n\nDo you want to try it again ?
1073	No system administrator password was defined.
1074	For twin boot mode Windows boot drive must be set to 'bootable'.
1075	Installation drive must be encrypted for twin boot mode.
1076	The uninstallation process has failed.\n\nAdditional information can be found in the file Sgeasy.log.
1077	Uninstallation of GINA system has failed.
1078	New drivers and services have been installed. We now strongly recommend that you create a new backup, because you cannot use your old backups for restore while SafeGuard Easy is installed!
1079	Uninstallation of GINA client SGEGINA has failed.
1080	Removing a system menu entry has failed.

1081	Removing a system menu entry has failed.
1082	Entry in INI file not found.
1083	Installation of Cardman API has failed.
1084	For twin boot mode the kernel drive must be encrypted.
1085	For twin boot mode at least one startable drive must not be encrypted.
1086	A complete [PN] system is still installed\non your computer on another operating system platform. You need to uninstall this system\nbefore you can uninstall the runtime system from the current operating system.
1087	Installation of a [PN] system is not allowed.
1088	A required PBA resource file (.MOD) could not be found!
1089	The installation of [PN] could not be completed\n\ndue to the following error:\n\n%1\n\nPlease press the OK button to remove all installed components of the\n[PN] system.\n\nAfter that an automatic system reboot will be performed.
1090	Wrong version of operating system found.\n\nOperating system Windows NT v4.00 is required.
1091	Wrong version of operating system found. \n\nOperating system Windows 95/98/ME is required.
1092	The uninstall procedure cannot be started because one or more [PN] components are currently not running.
1093	This process cannot be executed because an encryption operation is currently running. Please wait until all encryption operations are completed and start this program again.
1094	Uninstallation process is running. Administration is no longer allowed.

1095	Maximum number of hard disks exceeded. \nInstallation of [PN] is not supported on this system.
1096	Some non-DOS partitions were found which would be encrypted next using this install type.\n\nTherefore we recommend that you choose install type'Partitioned'.
1097	Wrong version of operating system found. \n\nOperating system Windows 2000 is required.
1098	Installation of SafeGuard Easy has failed.
1099	Uninstallation of SafeGuard Easy has failed.

Common errors

1101	Self check failed.
1102	Help system could not be initialized.
1103	Class could not be registered.
1104	The partition configuration information is inconsistent.
1105	Invalid or wrong parameter defined.
1106	No, or not, enough parameters were defined.
1107	Unknown parameter defined.
1108	Not enough memory available.
1109	Module '%1' could not be loaded.
1110	Dialog could not be created.
1111	Dialog could not be initialized.
1112	Thread could not be created.
1113	Window could not be created.
1114	You need administrator rights to install or uninstall.
1115	An access violation has occurred!
1117	Log file '%1' could not be opened.
1118	You cannot run the Uninstall and Administration programs of [PN] at the same time. \n\nPlease quit the currently running program before you start another.

1119	Kernel file not found.
1120	Installation of control handler failed.
1121	Unknown environment variable defined.
1122	Environment variable could not be set.
1123	Buffer too small.
1124	The dynamic link library '%5' couldn't be loaded.
1125	The specified function '%5' couldn't be found.
1126	The semaphore '%5' couldn't be opened.
1127	The module '%5' couldn't be release.
1128	An exception has occurred during execution of a\n [PN] subsystem function.\n\nLast error code : %1\nFunction return code: %2\nModule : %3\nLine number : %4\nAddress : %5\n\nPlease contact Utimaco Safeware AG!
1129	A critical error has occurred during the execution\nof one or more [PN] subsystem functions.\n\nFatal error code: %1\nOS error code : %2\nModule : %3\nFunction : %4\n\nDescription: [[MSGLINK]=%1].
1130	Allocated memory could not be released.
1131	Function is currently not supported.
1132	Access denied.
1133	Failed to start program '%1'.
1134	Function or resource is not available.
1135	Process was aborted by user.
1136	Invalid or wrong entry defined.
1137	System is currently changing some system settings. New changes are currently not allowed.
1139	Invalid data type for dialog field
1141	Kernel backup failed.
1143	Defined workstation does not exist

1144	The logon client 'SgeGina.dll' could not be found. This component provides vital functionality of [PN]. Removing or disabling it can cause serious problems that may require you to reinstall [PN] or the operating system.
1145	The 'SgeCtl.exe' service could not be found. This component provides essential basic functionality for [PN]. Removing or disabling it can cause serious problems that may require you to reinstall [PN] or the operating system.
1146	The system kernel is corrupted!
1147	A hard disk partition encryption or decryption is currently performed or such a process was initialized.\nYou can only make a kernel backup if all pending encryption or decryption processes are completed.
1148	The interface couldn't be found on the system.\n\nClass identifier:%1 (%3)\nInterface :%2\nhResult :%4 ([[OSERRLINK]=%5])\n\nIt is possible that [[FILELINK]=SGE_INFO.DLL][[MSGLINK]=102] is not installed on '%6'!

Configuration file errors.

1151	Configuration file %1 could not be found.
1152	No configuration file defined.
1153	Invalid configuration file.
1154	Invalid entry in configuration file found.
1155	Configuration file %1 could not be created.
1156	Error found in line %1 of the configuration file.
1158	The specified configuration file couldn't be found!
1159	An unknown command was found in the configuration file.

1160	An unknown configuration file type was detected.
1161	The type of the configuration file is not valid.
1162	Handle for the configuration file could not be created.
1163	Configuration file for uninstallation could not be created.
1164	Configuration file for installation could not be created.
1165	Configuration file %1 could not be found.
1166	The type of the configuration file is not valid.
1167	Execution of the configuration file '%1' failed.

MESSAGE control errors.

1171	Message ID %1 not found.
1172	No control text for control ID found.
1173	The Windows NT event log couldn't be written.
1174	An invalid file or message link command was found:\n\nMessage identifier: %1\nLink command : %2.
1175	The format of the given message file '%1' is invalid.
1176	Wrong definition of message box attributes

Password errors

1181	No system administrator password defined.
1182	The password is incorrect. Please retype your password.
1183	No password defined.
1184	Defined password is too short.
1185	Defined password is too long.
1186	Defined passwords do not match.

1187	The password is trivial.\nDo you want to enter a different one?
1188	The password already exists for another user. \nDo you want to use this password anyway?
1189	The password does not contain the required number of characters, othercase characters, numeric characters and symbols.
1190	The password has not yet reached its defined minimum age.

Key errors

1201	A hard disk key is not yet defined.\n\nSetting encryption for hard disk partitions is not allowed\nas long as no key is defined for hard disk drives.
1202	A floppy disk key is not yet defined.\n\nSetting encryption for floppy disk drives is not allowed\nas long as no key is defined for floppy disk drives.
1203	A removable disk drive key is not yet defined.\n\nSetting encryption for removable disk drives is not allowed\nas long as no key is defined for these drives.
1204	Defined key is too long.
1205	Defined key is too short.
1206	The defined keys do not match.
1207	No key was defined.
1208	The Boot Protection mode requires\nan encryption key for the hard disk.
1209	The Standard mode requires an\nencryption key for the hard disk.
1210	The key is trivial.\nDo you want to enter a different one?

IPC errors

1221	IPC server could not be started.
1222	IPC client could not be started.
1223	IPC connection could not established.
1224	IPC message could not be fetched.
1225	IPC message could not be posted.
1226	IPC function IPC_SGE_PROCESS_DEF_MSG\ncould not be processed.
1227	IPC server could not be closed.
1228	IPC client could not be closed.
1229	IPC thread could not be started.
1230	Waiting for IPC message failed.
1231	IPC communication object not found.

Drive errors

1241	Unknown or invalid drive defined.
1242	No more drives found.
1243	Drive I/O operation has failed.
1244	Reading from a drive has failed.
1245	Writing to a drive has failed.
1246	Access to a drive has failed.
1247	Drive is not ready.
1248	Locking a disk drive has failed.
1249	Unlocking a disk drive has failed.
1250	The system partition must be a primary partition.\n\nFor example this is required if the 'Support for Compaq setup partition' option is defined.

1251	Dismount of volume has failed.\n\nMaybe some files or windows from volume are still open.
1252	The first physical disk is not a hard disk drive.
1253	All entries in partition table of MBR sector on the first hard disk are already used.\n\nOption 'Support for Compaq setup partition' requires a free, unused partition table entry!
1254	System has started in compatibility mode.
1255	To install SGE, please remove your hot pluggable hard disk.
1256	No drives of this type are available.
1257	Internal error accessing system partition

SERVICE errors

1261	Info about a memory object for a system service \ncould not be released.
1262	Error detected in system service dispatcher.
1263	System service could not be started.
1264	System service status could not be changed.
1265	Handler for system service could not be registered.
1266	The service initialization function reported an error.
1267	The service information block couldn't be found.\nThere is probably not enough memory available.\n\nErrorcode: %1.

REGISTRY errors

1271	Entry in the registry could not be opened.
1272	Entry in the registry could not be read.
1273	Entry in the registry could not be written.
1274	Entry in the registry could not be created.

1275	Entry in the registry could not be removed.
1276	Entry for system service in the registry \ncould not be opened.
1277	Entry for a system service in the registry \ncould not be created.
1278	Entry for a system service in the registry \ncould not be removed.
1279	Entry for a system service in the registry \nalready exists.
1280	Could not open Session Control Manager.
1281	Entry in the registry for a session \ncould not be found.
1282	Invalid entry in the registry detected.

Driver database file errors

1291	No more encryption drivers found.
1292	Driver database file not found.
1293	Error occurred while reading the driver database file.
1294	Driver database file is empty.
1295	Illegal or invalid entry in driver database file.

CRAREA errors

1301	Installation drive cannot be accessed.
1302	Request of partition information failed.
1303	Access to boot partition failed.
1304	Invalid process option defined.
1305	Unknown or invalid file system defined.
1306	Difference between type of current file system \nand type of defined file system detected.

1307	Difference between current cluster size and \ndefined cluster size detected.
1308	Invalid start cluster for kernel area defined.
1309	Invalid start sector for kernel area defined.
1310	Invalid partition type defined.
1311	No free clusters for kernel found .
1312	Clusters could not be marked as 'Used'.
1313	Clusters could not be marked as 'Good'.
1314	Clusters could not be marked as 'Unused'.
1315	Clusters could not be marked as 'Bad'.
1316	Cluster information is corrupt.
1317	Area marked as "Bad" could not be found.
1318	Invalid size of kernel area defined.
1319	MBR sector on 1st hard disk could not be replaced.

SGOCA Errors

1401	The requested object communication area information data already exists.
1402	The object communication area already exists.
1403	The requested object communication area information data already exists.
1404	The object communication area couldn't be found.
1405	The requested object communication area information data doesn't exist.
1406	Additional object information data found.

SGUICL Errors

1511	The applications component configuration database can't be loaded!

ADMLOGON errors

1601	The logon failed. Please retry.
1602	The [PN] subsystem does not allow more than 5 logon attempts. You must restart your computer to start this application again.
1603	The start of the [PN] logon component has failed.
1604	
1605	The logon to [PN] was successful, but you \ndon't have sufficient rights to uninstall the product.

Administration errors - USER

1801	User '%1' cannot be created because \nthe maximum count of users has been exceeded.
1802	It is not possible to create or delete the '*AUTOUSER'.
1803	User '%1' already exists. Please specify another user identification name.
1804	The maximum count of users has been exceeded.
1805	You are not permitted to create or delete the 'SYSTEM' \nuser profile. You can only modify this profile.
1806	The user profile used requires a token to authenticate to [[FILELINK]=SGE_INFO.DLL][[MSGLINK]=102].
1807	The application has been blocked for more than 30 seconds, because it is waiting for a call to complete. In most cases this happens because the computer is busy. Do you want to wait until the application gets ready, or do you want break [cc]

Migration Wizard errors

2001	Migration Wizard could not be initialized

SGEGINA errors

2100	The Auto Logon failed.\n\nDo you want to edit the current relationship between the SafeGuard Easy user\nand the user of the operating system?
2101	You now need to change your password. \nThe Auto Logon (SAL) will be disabled for this login session!

Uninstall errors

2201	The uninstall procedure can’t be started because an encryption \nor decryption process is currently running!
2202	Deregistration of a component has failed!
2203	The uninstall procedure can not be proceeded because one or more foreign hard disk partitions are detected. Please remove the hard disk plugged in after the installation of [[MSGFILE]=SGE_INFO.dll][[MSGLINK=102].

Extended Installation errors

2301	The installation package has the wrong version number and could not be used!

2302	For installation mode ’Full disk encryption’ or ’Bootprotection’ no more than 8 partitions are allowed per hard disk!
2303	Registration of a component has failed!
2304	Installation of [PN] requires Microsoft’s Windows Installer!\nPlease read the manual or README file about how to install Windows Installer.
2305	Wrong version of operating system found.\n\nOperating system Windows NT/2000 is required.

Emergency Disk Wizard errors

2401	Creating the kernel backup file was cancelled!
2402	Not all emergency tools could be copied successfully!

SAL Errors

2501	Can’t open SAL-File
2502	The structure of the SAL - file is not correct
2503	Undefined errors occurred by file handling
2504	Errors occurred by positioning the SAL - file
2505	SAL file read error
2506	SAL file write error
2507	The specified user can’t be found
2508	No current user found
2509	Write into the SAL file fails. The existing record should be the same size.
2510	The target buffer is too small for the entire record
2511	No memory allocation

Database error

2601	Writing of data to database has failed !
2602	Reading data from database has failed!
2603	Creating a database entry has failed!
2604	Deleting a database entry has failed!
2605	Database is not available!

Interface Error

3001	The specified COM Interface couldn't be encrypted.\nInterface name:%1\nError number: %2\n\nDetailed Information:\n%3
3002	The execution of an interface method has failed. The following detailed information is available:\nError number: %1\nhResult: %2\nDescription: %3\nInterface :%4\nPlease contact your system administrator!

Client/Server errors

3201	Server or client is currently busy and is not able to process the request.

Administration Console Errors

3301	Database connection failed!
3302	Server Console Interface not found!
3303	Remote Administration Interface not found!
3304	Configuration File Wizard Interface not found!